Biblioteca profesional

MANUAL DE CISCO

Cuarta edición

- Obtenga una introducción completa a las tecnologías y los productos de Cisco.
- Aprenda a trabajar con enrutadores, conmutadores, concentradores y software de Cisco.
- Obtenga una cobertura amplia sobre VoIP, redes de área de almacenamiento (SAN) y redes de distribución de contenido (CDN).
- Implemente soluciones de seguridad en redes.

McGraw Hill

Toby Velte

Manual de Cisco®

Cuarta edición

TOBY J. **VELTE**
ANTHONY T. **VELTE**

Traducción
Carlos Cordero Pedraza
Catedrático
Secretaría de Marina y Armada de México, CESNAV

Jorge Arturo Pineda Sánchez
Traductor profesional

MÉXICO • BOGOTÁ • BUENOS AIRES • CARACAS • GUATEMALA • LISBOA • MADRID
NUEVA YORK • SAN JUAN • SANTIAGO • AUCKLAND • LONDRES • MILÁN
MONTREAL • NUEVA DELHI • SAN FRANCISCO • SINGAPUR • SAN LUIS • SIDNEY • TORONTO

Director Editorial: Fernando Castellanos Rodríguez
Editora de desarrollo: Cristina Tapia Montes de Oca
Supervisora de producción: Jacqueline Brieño Álvarez
Formación editorial: María Alejandra Bolaños Avila

MANUAL DE CISCO. Cuarta edición

Prohibida la reproducción total o parcial de esta obra,
por cualquier medio, sin la autorización escrita del editor.

McGraw-Hill Interamericana

DERECHOS RESERVADOS © 2008, respecto a la cuarta edición en español por
McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.
A Subsidiary of ***The McGraw-Hill*** *Companies, Inc.*
Prolongación Paseo de la Reforma 1015, Torre A,
Pisos 16 y 17, Colonia Desarrollo Santa Fe,
Delegación Álvaro Obregón,
C.P. 01376, México, D. F.
Miembro de la Cámara Nacional de la Industria Editorial Mexicana, Reg. Núm. 736

ISBN-13: 978-970-10-5927-2
ISBN-10: 970-10-5927-1

Traducido de la cuarta edición de
Cisco®: A Beginner's Guide, Fourth Edition
By: Toby J. Velte and Anthony T. Velte
Copyright © MMVII by McGraw-Hill/Osborne. All rights reserved

ISBN: 0-07-226383-0

4123567890 0976543218

Impreso en México *Printed in Mexico*

The McGraw-Hill Companies

Este libro está dedicado
a nuestras madres, padres, esposas
e hijos.
Ellos nos han traído realmente las más grandes
de nuestras riquezas.

ACERCA DE LOS AUTORES

Toby J. Velte, doctor en física, socio certificado de redes de Cisco, es un autor internacional de libros y artículos que han alcanzado grandes ventas sobre tecnología de negocios. Es cofundador de Velte Publishing, Inc. y coautor de algunos libros publicados por McGraw-Hill y Cisco Press.

En la actualidad es parte de Accenture's North American Products.

Anthony T. Velte, profesional certificado de seguridad en sistema de información, socio certificado de sistemas de Cisco, socio certificado de diseño de Cisco y auditor certificado de sistema de información, cuenta con más de 16 años en la industria de los sistemas de información. Es cofundador de Velte Publishing, Inc. y coautor de algunos libros publicados por McGraw-Hill y Cisco Press.

El señor Velte cuenta con varias certificaciones, entre las que se incluyen profesional certificado de seguridad en sistema de información (CISSP) y auditor certificado de sistema de información (CISA). Asimismo, es miembro asegurado de la FBI Infragard Minnesota Membership Alliance (IMnMA).

Acerca del editor técnico

Wesley J. Noonan (Houston, Texas) ha trabajado en la industria de la computación desde mediados de la década de 1990, especializándose en redes basadas en Windows y en la implementación y el diseño de la seguridad de la infraestructura de redes. Es ingeniero de calidad de Attachmate, y trabaja en la línea de productos relacionada con las soluciones de seguridad de la compañía. Wes es el autor de *Hardening Network Infraestructure* y es coautor y ha contribuido en los libros *The CISSP Training Guide* de la editorial QUE Publishing, *Hardening Network Security* de McGraw-Hill y *Firewall Fundamentals* de la editorial Cisco Press. Wes también ha contribuido en la revista *Redmond*, escribiendo acerca de temas de seguridad e infraestructura de redes. Wes mantiene una sección "Pregúntele a los Expertos" en Techtarget.com (http://searchwindowssecurity.techtarget.com/ateAnswers/0,289620,sid45_tax298206,00.html) relacionada con la seguridad de redes de Windows.

UN VISTAZO AL CONTENIDO

Parte I Panorama general de Cisco

▼ 1 Cisco e Internet 3
▼ 2 Introducción a las redes 29

Parte II Herramientas de Cisco para la interconectividad

▼ 3 Revisión general de los enrutadores 89
▼ 4 Configuración de enrutadores 137
▼ 5 Conmutadores 187
▼ 6 Panorama general de la seguridad 243
▼ 7 Los bloques de construcción de la seguridad 285
▼ 8 Soluciones inalámbricas de Cisco 333

Parte III Soluciones de negocios de Cisco

▼ 9 Centro de contacto unificado de Cisco 379
▼ 10 Herramientas de almacenamiento..... 409
▼ 11 Redes de contenido y soluciones de video de Cisco..... 437

Parte IV Diseño de redes de Cisco

▼ 12 Protocolos de enrutamiento..... 475
▼ 13 Administración de red..... 521
▼ 14 Procesos de diseño de redes 571
▼ 15 Detección y solución de problemas en redes de Cisco..... 617

▼ Índice 663

CONTENIDO

Parte I

Panorama general de Cisco

▼ 1 Cisco e Internet 3

Interconectividad 4

La posición de Cisco en la industria de la computación 6

El panorama de Internet 8

Productos de Cisco 20

Competencia 20

¿Quién desea ser millonario? 21

Soluciones de Cisco 25

▼ 2 Introducción a las redes 29

Bits y bytes 30

Cómo interpretan los datos las computadoras 30

Modelo de referencia OSI 34

La pila de siete capas 34

Implementación OSI por capa 37

Tecnologías de red 39
Ethernet 39
Gigabit Ethernet y 10 Gigabit 41
Token Ring 42
ATM 44
FDDI 45
Inalámbrico 47
Tecnologías WAN 48
Tecnología de marcado telefónico 49
Tecnologías troncales WAN 52
TCP/IP 55
Mensajería TCP/IP 57
La capa de transporte 61
Direccionamiento IP 66
El formato de las direcciones IP 67
Clases de direcciones IP 69
Direccionamiento privado 71
Subredes 71
Versión 6 de IP 79
Integración 84

Parte II

Herramientas de Cisco para la interconectividad

▼ 3 Revisión general de los enrutadores 89
Cómo trabajan los enrutadores 91
Enrutamiento para lograr mayor eficiencia 92
Los enrutadores e Internet 93
Enrutadores ópticos 95
Comunicación con un enrutador 98
El puerto de consola 100
El puerto auxiliar 101
Telnet 102
La interfaz de usuario del servidor HTTP 103
Administrador de dispositivos de seguridad 105
Seguridad de los enrutadores 110
Contraseñas de enrutadores 112
El hardware del enrutador 116
Memoria del enrutador 117
Puertos y módulos del enrutador 119
Modelos de enrutadores Cisco 122
Archivos esenciales 126
El IOS: el sistema operativo de las interconexiones 127
El archivo de configuración 134

▼ 4 Configuración de enrutadores 137
El papel primordial del archivo de configuración 138
Tres tipos de archivos de enrutadores Cisco 139
Comience a trabajar con los enrutadores Cisco 142
Comunicación con el IOS 142
Conozca el IOS 12.4 143
Conozca IOS XR 147
Utilización de los comandos del IOS 148
Revisión general de los modos del enrutador 154
Comandos básicos del enrutador 157
Configuración paso a paso de un enrutador 158
Modo de configuración 159
Asignación de una identidad a un enrutador 163
Examen del estado de un dispositivo 165
Protocolo de descubrimiento de Cisco 165
Recuperación de contraseñas 169
Recuperación de las Enable Passwords 169
Recuperación de contraseñas de enrutadores Cisco anteriores ... 173
Utilización de aplicaciones para ayudar a configurar enrutadores .. 174
ConfigMaker 175
Fast Step 180

▼ 5 Conmutadores 187
Topologías de las redes 189
La importancia de los dominios de red 193
El cableado define la velocidad y distancia de la red 197
Conmutadores Cisco 205
Cómo funciona un conmutador individual 205
Fundamentos de la conectividad conmutada 206
Diseño de interconexiones conmutadas 209
VLAN 213
Productos de Cisco para redes conmutadas 215
Configuración y administración de los conmutadores de Cisco 218
Cluster Management Suite (CMS) 219
Software del Cluster Management Suite 222
Página inicial de la Cluster Management Suite 222
El dispositivo gráfico en la Cluster Management Suite 223
Topology View (Vista de la topología) 224
Configuración del puerto del conmutador 226
Agrupamiento de puertos 228
Monitoreo de puertos (SPAN) 229
Controles para inundación/puertos de red 230
Administración IP 230

Configuración SNMP 231
Tabla ARP 233
Administración de direcciones 234
Seguridad de los puertos 235
Cisco Group Multicast Protocol (protocolo de transmisión múltiple de grupo de Cisco) 236
Spanning-Tree Protocol (protocolo de árbol expandido) 238
Membresía VLAN 239
Administración del VTP 240
Configuración del VMPS 240

▼ 6 Panorama general de la seguridad 243

Panorama general de la seguridad de las redes 246
Seguridad basada en el tráfico 246
Seguridad basada en el usuario 248
Autentificación, autorización y contabilidad 252
Panorama general del modelo AAA 252
Cómo trabaja el AAA 259
Listas de acceso dinámico 281
Cerradura y llave con una base de datos local de usuario 282

▼ 7 Los bloques de construcción de la seguridad 285

Firewalls 287
Fundamentos de los firewalls 287
Cómo funcionan los firewalls 291
El conjunto de características del firewall del IOS 301
Firewall PIX Secure de Cisco 311
Aparatos adaptivos de seguridad 319
Redes privadas virtuales 322
¿Qué compone una VPN? 322
La solución de Cisco 325
Enrutadores de acceso 329
Panorama general 330
Modelos 331
Conjunto de administración de la seguridad de Cisco 331
Cisco Security Manager 332
MARS de Cisco Security 332

▼ 8 Soluciones inalámbricas de Cisco 333

Introducción a la conectividad inalámbrica 334
Las raíces de la conectividad inalámbrica 334
Beneficios 335
WLAN 337
Cómo trabajan 337

Arquitectura 339
Tecnologías 342
Conectividad inalámbrica de Cisco 350
Filosofía 350
Productos de Cisco 351
Configuración de los puntos de acceso 355
Estudio del sitio 356
Colocación del punto de acceso 357
Interferencia 357
Configuración inicial 358
Seguridad 361
Colocación de las antenas 367
Configuración del cliente 367
Instalación 367
Configuración 368

Parte III

Soluciones de negocios de Cisco

▼ **9** Centro de contacto unificado de Cisco 379
VoIP 380
Introducción 381
Desarrollo de redes VoIP 382
H.323 391
SIP 395
SCCP 397
Implementación 397
Cisco Unified Communications (comunicaciones unificadas de Cisco) 400
"Esto lo cambia todo" 400
Cisco Unified Presence Server (servidor de presencia unificada de Cisco) 401
Soporte SIP 402
Productos y componentes 403

▼ **10** Herramientas de almacenamiento 409
Redes de área de almacenamiento 411
Necesidades de almacenamiento 411
Fibre Channel 412
Otros protocolos SAN 415
Diseño y construcción de una SAN 416
Conmutadores y directores Cisco MDS 421
Tecnologías 421

Hardware 427
Software 431
Almacenamiento adjunto de red 433

▼ **11** Redes de contenido y soluciones de video de Cisco 437
Redes de entrega de contenido 438
Introducción a las CDN 438
La solución de Cisco 441
ACNS 450
Motor de aplicación de área amplia 451
Sistema de archivos de área amplia 452
Almacenamiento en el caché 453
Protocolo de comunicación de la caché Web 455
Actualización 456
Almacenamiento en caché de los motores de contenido 457
Soluciones de video de Cisco 465
Scientific-Atlanta 465
Solución de video para negocios de Cisco 466
Solución de videoconferencia IP 468
Sistema de medios digitales 470

Parte IV
Diseño de redes de Cisco

▼ **12** Protocolos de enrutamiento 475
Revisión general de los protocolos de enrutamiento 476
Fundamentos del protocolo de enrutamiento 477
Arquitecturas de protocolo de enrutamiento 495
Cómo se implementan los protocolos de enrutamiento 500
Revisión de los protocolos de enrutamiento de Cisco 506
Protocolo de enrutamiento de gateway interior de Cisco 506
Configuración del RIP 2 512
Configuración de Open Shortest Path First 513
Protocolo de gateway de borde 514
Conmutación de etiquetas de varios protocolos 517
Estrategia de los protocolos de enrutamiento de Cisco 519

▼ **13** Administración de red 521
Revisión general de la administración de red 523
La evolución de las herramientas de administración 524
Herramientas de la administración de redes hoy en día 526
Tendencias en la administración de sistemas empresariales ... 529
SNMP es una plataforma de administración común IP 531
¿Qué es SNMP? 531

Encuestas SNMP y objetos administrados 532
La MIB 534
Encuestas de grupos y agregación de datos 539
Comandos SNMP 542
Umbrales 542
Eventos y trampas 543
RMON: sondas de hardware para redes conmutadas 545
Tendencias en la tecnología de administración de red 548
SNMP de Cisco e implementaciones RMON 552
Cisco Network Assistant 555
Características 556
Instalación 556
Vistas 557
Interacción 559
Comunidades 561
Uso de CNA 564

▼ **14** Procesos de diseño de redes 571
Fundamentos del diseño de interconexiones 572
Revisión de los fundamentos de las interconexiones 572
El modelo de diseño jerárquico de tres capas 578
Métodos de diseño 583
Diseño para satisfacer las necesidades 588
Comprensión de las redes existentes 590
Caracterización de las redes 591
Diseño de red de Cisco 596
Diseño lógico de la red 596
Diseño de red en campus 601

▼ **15** Detección y solución de problemas en redes de Cisco 617
La mecánica de la detección y solución de problemas en redes 618
Métodos para detección y solución de problemas en redes 619
Detección y solución de problemas de IP de host 622
Aislamiento de problemas de conectividad 625
Detección y solución de problemas de vínculos WAN 641
VPN cliente-servidor 646
Detección y solución de problemas del hardware de Cisco 649
Inspección de dispositivos 649
La prueba de reinicio 651
Detección y solución de problemas de configuraciones de red 651
Redes inalámbricas 652
Detección y solución de problemas de rendimiento de red 659

▼ Índice 663

PREFACIO

Es raro que un libro técnico tenga la vigencia suficiente para obtener siquiera una segunda edición, ¡ya no digamos una cuarta! Esta edición es un buen reflejo de la utilidad del libro y el deseo de sus autores de mantenerlo actualizado. No sólo encontrará los fundamentos necesarios para aprender cómo trabajan las redes, sino que también encontrará información acerca de novedosas soluciones de conectividad. Desde los fundamentos de cómo funcionan las redes hasta los principios necesarios para un buen diseño y seguridad, este libro abarca todas las bases que necesitará para tener éxito en el campo de las redes.

El estudio de la tecnología inalámbrica, voz sobre IP, enrutadores, conmutadores, firewalls y todas las interacciones asociadas es un aspecto importante en los ambientes de cómputo cada vez más complejos y críticos. Las redes ya no son sólo la espina dorsal de las comunicaciones, sino que también lo son de los negocios. La comprensión de cómo se llevan a cabo los negocios en este ambiente es crucial; ser parte de un equipo que pueda trabajar, utilizar, resolver fallas y diseñar redes de negocios es fundamental para el éxito en estos días.

Incluso muchos profesionales que trabajan en el campo no poseen un conocimiento profundo de la tecnología inalámbrica, autentificación y firewalls. En realidad, mantenerse actualizado con las implementaciones de seguridad de Cisco puede ser un trabajo de tiempo completo. Por fortuna, los autores llevaron a cabo la parte complicada por usted: reunir toda la información que necesitará para comprender las tecnologías de punta y cómo hacer que éstas funcionen en la realidad.

Como "persona dedicada a la seguridad", estoy muy sensibilizado ante la cobertura de este libro. Esta industria necesita cada día más gente que comprenda cómo funciona una buena seguridad, cómo utilizarla y, lo más importante, cómo administrarla. En la actualidad, proteger la red de una organización significa mantenerla en el negocio. Desde las redes militares y gubernamentales hasta las de compañías, escuelas y organizaciones sin fines de lucro, la infraestructura básica es la misma. Este libro le ayudará a comprender y utilizar esa infraestructura. Desde los principios fundamentales del diseño de las redes hasta la autorización de usuario, éste es un estudio real de principio a fin de la base de la información y de la red de telecomunicaciones emergente.

Aunque el eje de este libro es el equipo de Cisco, los fundamentos y las bases para configurar, diseñar y utilizar las redes siguen siendo las mismas sin importar qué proveedor seleccione. Indudablemente, Cisco es el líder y, por tanto, el requisito principal para su uso es que conozca Cisco, pero este libro le ayudará a comprender la tecnología sin importar qué proveedor elija usted o su empresa.

Cómo funcionan, cómo diseñarlas, cómo administrarlas, cómo mantenerlas fuera de peligro, cómo utilizar la última tecnología de manera eficiente (este libro le proporcionará todo lo que desee saber para tener éxito en el mundo interconectado de hoy).

En la actualidad, casi todo mundo ha utilizado las redes computacionales para comprar artículos, comunicarse con personas de todo el mundo, enterarse de eventos actuales e investigar acerca de sus intereses. Ahora puede dar el siguiente paso y aprender cómo trabaja todo esto y cómo diseñar nuevas redes. Este libro es un gran paso para emprender una nueva e interesante carrera.

A pesar de que han pasado más de 20 años desde que instalé mi primera red de área local para la agencia de comunicaciones de la Casa Blanca, aún percibo una gran sensación de logro cuando instalo una red de principio a fin. Trabajar en la conectividad de redes me ha llevado desde los círculos de poder, hasta los grandes negocios, a la seguridad de la información y a construir mi propio negocio. A pesar de que los viejos cables coaxiales de mi primera red ya no se usan, y la fibra y los cables de cobre de alta capacidad de mi próxima red apenas se están instalando, la importancia que le doy a la gente que utiliza mis redes no ha cambiado en lo más mínimo.

Paul D. Robertson
Moderador: Firewall-Wizards
Fundador: FluidIT Group (www.fluiditgroup.com)

AGRADECIMIENTOS

La primera edición de este libro no hubiera podido llevarse a cabo sin la enorme contribución del autor Tom Shaughnessy. A él le debemos las maravillosas bases sobre las cuales construir. En la segunda, tercera y cuarta ediciones, agradecemos los talentos del autor Robert Elesenpeter. Él corrigió los errores de mecanografía, editó y reorganizó las partes de texto y artística para que fueran claras y actualizadas, y contribuyó con trabajos originales en las tres ediciones. Asimismo, expresamos nuestro agradecimiento a Wes Noonan, nuestro editor técnico, quien de una manera seria, se hizo responsable de asegurar la precisión técnica de este libro.

Fue un verdadero placer trabajar de nuevo con el equipo de McGraw-Hill. A la editora ejecutiva, Jane Brownlow, y a la coordinadora de compras de esta edición, Jennifer Housh, y a todos los demás miembros del equipo de producción de McGraw-Hill, les decimos muchas gracias.

Por último, quisiéramos extender nuestro agradecimiento a Ian Stong de ccie4u.com. Él nos proporcionó el acceso en línea a una gran variedad de información de Cisco que se utilizó para terminar esta edición. No cabe la menor duda de que ccie4u.com y servicios como éste, son un recurso muy valioso para el principiante, para alguien que desea obtener una certificación avanzada y hasta para un par de personas que trabajan en una *Guía para el principiante* de Cisco. De modo que si por alguna razón necesita acceder a gran cantidad de información de Cisco, consulte el sitio ccie4u.com.

INTRODUCCIÓN

El volumen que tiene en sus manos es la cuarta edición de introducción a la conectividad de Cisco mejor vendida en el mundo. Desde que este libro se presentó por primera vez, se han vendido más de 60 000 copias, se ha traducido a muchos idiomas y se ha distribuido por todo el mundo. Este nivel de interés confirma lo que ya sabe (Cisco es, y seguirá siendo, un gran jugador en la industria de las comunicaciones, y la gente quiere comprender mejor cómo funciona este gigante).

A pesar de que han transcurrido dos años desde que se escribió la tercera edición, este libro ha seguido siendo muy popular y sentimos que era necesario realizar una nueva edición e igualmente que con la tercera edición, se reexaminaron cada uno de los capítulos. Aunque fue difícil encontrar material que pensamos que ya no era conveniente incluir, encontramos nuevos temas que teníamos que tratar. Por ejemplo, Cisco ha lanzado sus productos de voz sobre IP (VoIP) con su reciente solución Cisco Unified Communications. Era necesario incluir en el libro esta tecnología y línea de productos totalmente nueva. En la tercera edición, se expandió la cobertura de soluciones de negocios de Cisco, incluidos VoIP, redes locales de almacenamiento (SAN) y redes de distribución de contenido (CDN). Puesto que este contenido sigue evolucionando, continuamos expandiendo la cobertura en los tres capítulos. Asimismo, debido a que la conectividad inalámbrica ha dado un paso enorme, esa sección se ha modificado también. Debido a que la seguridad ha cobrado gran importancia, incluimos también una sección acerca de seguridad. Desde luego, todos los capítulos se actualizaron para cubrir los últimos productos de software y hardware de Cisco.

Así que, ¿cuál es la razón de todo este trabajo y revisión? Seguimos pensando que existe una necesidad enorme por parte de los profesionales en conectividad de una introducción clara y concisa a Cisco y su tecnología. Lo que en realidad se necesita es una comprensión simple de la conectividad y el papel que juega Cisco en dicha conectividad para que tengan sentido muchos problemas acerca de las tecnologías de la información.

QUIÉN DEBE LEER ESTE LIBRO

Este libro está diseñado para cualquier persona que sea principiante en el campo de la interconectividad. Abarca lo que se conoce como la infraestructura técnica de Internet. El software sobre su escritorio (el navegador Web, el software FTP o el Messenger ICQ) es sólo la punta del iceberg. En los últimos 30 años, un grupo cada vez más grande de científicos en computación, ingenieros en telecomunicaciones y programadores ha estado muy ocupado en el diseño y la construcción de una infraestructura global que está revolucionando la cultura y los negocios de la misma forma. La interconectividad de redes ha adoptado su propio lenguaje por sí misma (aparte del que se utiliza en la industria de la computación).

Este libro es para aspirantes a profesionistas, interesados en aprender acerca del gigante de la conectividad, para gerentes de la industria de la computación cuyo conocimiento acerca de la interconectividad de redes es limitado, para profesionales en plataformas computacionales y software, y aun para personas con un interés en la tecnología.

Este libro es para los interesados en Internet y la interconectividad, no sólo en Cisco. Los fundamentos tecnológicos se estudian antes de profundizar en las particularidades de Cisco. Se utiliza Cisco en todos los ejemplos de este libro, porque cuenta con la línea de productos más grande y compleja en la industria y aún juega un papel muy importante en este campo.

Para los lectores interesados en obtener la certificación de Cisco, la lectura de este libro los familiarizará con los antecedentes de esta industria y con los conceptos, los términos y la tecnología. Después podrán continuar con un libro de preparación para el examen para pulir su examen CCNA. La guía más popular es, ciertamente, el libro para la preparación de la prueba CCNA, el *CCNA Cisco Certified Network Associate Study Guide*, *Deluxe Edition*, escrito por Todd Lammale.

QUÉ ABARCA ESTE LIBRO

A continuación se presenta un desglose capítulo por capítulo del contenido de este libro.

Parte I, "Panorama general de Cisco"

Capítulo 1, "Cisco e Internet": Internet representa el cambio económico más grande y rápido en la historia y tarde o temprano nuestras vidas se verán afectadas por esta tecnología (si es que aún no lo están). En este capítulo se analiza Internet como un fenómeno, poniendo particular énfasis en Cisco Systems y la manera en que su sistema operativo IOS ha elevado a la compañía a una posición que la coloca dentro de una élite en la industria de la computación, junto con Microsoft, Intel e IBM. Se proporciona un panorama general de la industria de la conectividad de redes y se explica cómo la línea de productos de Cisco compite por los nichos de la industria.

Capítulo 2, "Introducción a las redes": La tecnología moderna de conectividad es la culminación de docenas de tecnologías sofisticadas. En este capítulo se explican las cosas partiendo del cableado, comenzando con los electrones que circulan por los cables hasta los bits y bytes. Se proporciona una explicación de las principales tecnologías LAN como Ethernet y Token Ring, además de sus diferencias, cuáles se utilizan todavía y cuáles están en desuso, incluidas las tecnologías troncales de alta velocidad como ATM, Gigabit Ethernet y 10 Gigabit Ethernet. Se explica el modelo de referencia de siete capas para la interconexión de sistemas abiertos (OSI), incluido el funcionamiento interno del conjunto de protocolos TCP/IP (el software que utiliza Internet). Aprenderá la diferencia entre conectividad orientada a la conexión y no orientada a la conexión, además de la forma en que los nombres de dominio se traducen en direcciones IP numéricas. Se explican con detalle los fundamentos importantes del direccionamiento IP y las máscaras de subred. Se analiza la tecnología de ancho de banda como DSL e ISDN, además de las tecnologías troncales WAN como T1 y T3, Frame Relay y ATM.

Parte II, "Herramientas de Cisco para la interconectividad"

Capítulo 3, "Revisión general de los enrutadores": Este capítulo se concentra en los fundamentos de los enrutadores Cisco. Se estudian los componentes de hardware, desde las tarjetas de circuito impreso hasta las CPU, y se explica la forma como los administradores de red pueden ingresar a los enrutadores Cisco para trabajar en ellos, e incluso reinicializarlos para llevar a cabo tareas básicas como la recuperación de contraseña. Se analizan también los componentes principales del software de los enrutadores Cisco, incluida la interfase de comandos IOS y sus características. En esta parte se estudia la línea de productos de enrutadores Cisco, incluidos algunos consejos útiles acerca de cómo seleccionar el mejor enrutador para solucionar un problema de conectividad de redes en particular.

Capítulo 4, "Configuración de enrutadores": Es hora de adentrarse en el aspecto más difícil, especialmente el archivo de configuración. En este capítulo se analiza el modo de operación del IOS de Cisco, la jerarquía de comandos, las utilerías y cómo usar el subsistema de ayuda IOS. Pero el enfoque primordial está en el archivo de configuración, cómo se utiliza para instalar enrutadores Cisco y configurar redes. Al leer este capítulo se familiarizará con los comandos básicos del enrutador Cisco, la sintaxis de comandos y la forma como se lee el estado de los dispositivos y cómo configurar los parámetros clave del enrutador. Se revisan las herramientas de software de configuración ConfigMaker y FastStep de Cisco.

Capítulo 5, "Conmutadores": La *capa de acceso* es donde se conectan los dispositivos hosts como las PC y los servidores de interconexiones. En este capítulo se explican los fundamentos de la topología de red, las especificaciones de cableado, qué es el ancho de banda, qué diferencia a los dominios de colisión y de transmisión y en qué difieren los conmutadores de acceso y los concentradores. Asimismo se estudian los conmutadores de espina dorsal LAN desde la perspectiva de uno de los temas más importantes en la industria actual: si diseñar redes conmutadas o enrutadas. Se presentan los puntos de vista más técnicos de la conectividad conmutada, incluidos los protocolos de conmutación, las LAN virtuales (VLAN) y la conmutación multicapa. Se analizan las líneas de productos de conmutadores de Cisco.

Capítulo 6, "Panorama general de la seguridad": La seguridad de las redes que va más allá de los firewalls es seguridad basada en el usuario, y se utiliza para establecer y hacer valer las contraseñas para acceder a las redes y a las autorizaciones para hacer uso de los recursos de la red. En este capítulo se estudian en primera instancia los estándares industria-

les en que se basa la seguridad, en especial el estándar AAA (Authentication, Authorization and Accounting, autentificación, autorización y contabilidad). El estándar AAA se estudia al nivel de los comandos y después se repasa la línea de productos CiscoSecure ACS. Cisco ofrece dos productos de seguridad basados en el usuario: RADIUS, un estándar industrial y su propietario TACACS+. Ambos se estudian con todo detalle.

Capítulo 7, "Los bloques de construcción de la seguridad": Existen tres tipos de tecnologías para acceder a las redes: firewalls, servidores de acceso y redes privadas virtuales (VPN). En este capítulo se explican cada una de las tres, con un énfasis particular en los firewalls. Se explica la lista de acceso, así como los algoritmos adaptativos de seguridad de firewall, la tecnología que está en el corazón de la seguridad de las redes en el nivel del paquete. Cisco vende dos productos de firewall: la combinación hardware/software Cisco PIX Firewall y el software del conjunto de características IOS Firewall, ambos explicados con detalles. Se analiza la VPN (la WAN del futuro). También se estudia cómo funcionan los servidores de acceso y el papel que desempeñan. Además, se revisa la línea de productos de servidores de acceso de Cisco.

Capítulo 8, "Soluciones inalámbricas de Cisco": Hasta hace poco, la única forma de acceder a una red era mediante un cable delgado conectado a la parte trasera de su PC. Independientemente de lo eficiente que esto sea, fue sólo cuestión de tiempo hasta que a alguien se le ocurrió cómo eliminar el cable y permitir que los dispositivos se comunicaran entre sí a través de un medio inalámbrico. En este capítulo se estudian los fundamentos de la conectividad inalámbrica y después se profundiza en la solución de Cisco. La conectividad inalámbrica no es una tecnología sólo de "brujos"; conlleva todo el poder del cómputo y de la conectividad de redes a un rango de aplicaciones útiles y es benéfica en campos de aplicación como la salud y la educación. Cisco ofrece soluciones para LAN y WAN inalámbricas con su serie de productos Aironet y Airespace, que se expondrán, y más adelante se enseñará a configurarlos.

Parte III, "Soluciones de negocios de Cisco"

Capítulo 9, "Centro de contacto unificado de Cisco": Las redes y la conectividad de redes son una buena manera de transferir datos de un lugar a otro. Sin embargo, no sólo archivos de texto y estados de cuenta de las ganancias del cuatro trimestre pueden circular por la infraestructura de una red basada en productos de Cisco. Gracias a Voz sobre IP (VoIP), su organización puede utilizar su red como la espina dorsal de su sistema de telecomunicaciones. Además, los clientes que necesitan estar en contacto con su organización resultan beneficiados a partir de las comunicaciones unificadas de Cisco. Es una novedosa forma de utilizar VoIP que genera herramientas robustas y poderosas de voz, video e inteligencia.

Capítulo 10, "Herramientas de almacenamiento": Con los beneficios de la era de la información se genera un gran problema (¿dónde *almacenar* toda esa información?). En este capítulo, analizamos las redes de área de almacenamiento (SAN), que son parecidas a las LAN, pero se instalan con el objetivo de almacenar información. Hablaremos acerca del diseño y la instalación de las SAN, y después analizaremos la oferta de productos de Cisco para sus soluciones SAN, incluida su línea Multilayer Datacenter Switches (MDS, conmutadores de centro de datos multicapa).

Capítulo 11, "Rees de contenido y soluciones de video de Cisco": Las organizaciones están ofreciendo cada vez más información en sus sitios Web. Sin embargo, a medida que crece el número de personas que solicita esa información desde varios puntos, surge la ne-

cesidad de direccionar al cliente al punto de almacenamiento más cercano y de una manera rápida. Las redes de distribución de contenido (CDN) contribuyen a resolver el problema de la congestión en las redes, porque se proporciona a los clientes la información que necesitan desde el sitio ideal. En este capítulo se estudian los fundamentos de las CDN, junto con la línea de productos para esta tecnología de Cisco. Además, se estudia el tema de la memoria caché, una forma en que los proveedores de servicios y las grandes organizaciones pueden mantener información de acceso frecuente en Web, de manera que pueda enviarse al cliente sin tener que acceder a Internet repetidamente.

Parte IV, "Diseño de redes de Cisco"

Capítulo 12, "Protocolos de enrutamiento": Las grandes redes, o en este caso Internet, no serían posible sin los protocolos de enrutamiento. En este capítulo se estudian los problemas principales que enfrenta cualquier red, así como la forma en que los protocolos de enrutamiento se utilizan para adaptarse a los patrones de tráfico cambiantes, a los problemas que se presenten y a los cambios en la topología. En este apartado se estudia la tecnología de los protocolos de enrutamiento, además de los principales protocolos de enrutamiento que se utilizan en la actualidad: los protocolos estándar abiertos (RIP, OSPF, BGP) y los protocolos de propietario de Cisco (IGRP y EIGRP). Se estudian los protocolos de enrutamiento de Cisco a nivel comando, donde se establecen las mediciones de enrutamiento para modificar el comportamiento de la red y satisfacer los requisitos de la empresa.

Capítulo 13, "Administración de red": La administración de redes se ha convertido en un problema fundamental a medida que las redes han crecido en tamaño y complejidad. En este capítulo se estudian los estándares y las tecnologías de los sistemas de administración de redes: Simple Network Management Protocol (SNMP, protocolo simple de administración de redes), Remote Monitor Instrumentation (RMON, instrumentación de supervisión remota) y Management Information Base (MIB, base de información de administración). Se estudian los problemas relacionados con los estándares de administración de las redes, así como el método de implementación de dichos estándares que sigue Cisco. Se presenta la configuración SNMP en el nivel de comando. Se estudia también el grupo de productos de software de Cisco para la administración de redes (Resource Management Essentials y CWSI Campus).

Capítulo 14, "Procesos de diseño de redes": Existen fundamentos que deben tomarse en cuenta cuando se toma cualquier decisión de diseño de la red, ya sea para una red totalmente nueva o para una expansión modesta de una red existente. El modelo de diseño clásico jerárquico de tres capas se estudia en términos de qué tomar en cuenta en las capas de acceso, distribución y troncal. Se revisan los temas clave de diseño como la topología de red y el balance de tráfico. Se explica cómo llevar a cabo un análisis exhaustivo de las necesidades de la red y cómo traducirlo en soluciones de diseño utilizando productos de Cisco, cubriendo factores de diseño como los protocolos de enrutamiento, el diseño de direcciones, la comparación entre enrutamiento y conmutación, los servicios WAN y el balance de la carga de tráfico.

Capítulo 15, "Detección y solución de problemas en redes de Cisco": Se habrá convertido en un profesional en redes cuando pueda solucionar las fallas de una red. En este capítulo se analizan los problemas de las redes y la metodología apropiada para diagnosticarlos y repararlos. Se revisan los comandos clave para la resolución de fallas del IOS de Cisco en términos de cómo manejar problemas de conectividad, cuellos de botella, rendimiento de red y

otros problemas. Se pone particular atención al seguimiento y aislamiento de los problemas de configuración, afinación de las mediciones del protocolo de enrutamiento y solución de fallas en los servicios WAN, y de los vínculos de las líneas en serie. Además, se estudian problemas típicos en las redes inalámbricas, junto con la forma de reparar problemas relacionados con el desempeño de la red.

CÓMO LEER ESTE LIBRO

Se puede tomar este libro y empezar a leer desde el comienzo de cualquier capítulo. Los capítulos que estudian la tecnología comienzan desde los fundamentos y proporcionan explicaciones desde el punto de vista de los antecedentes históricos de dicha tecnología, de cómo evolucionó y de cuáles son los problemas y tendencias alrededor de la misma. Sólo hasta entonces se empiezan a estudiar los comandos IOS de Cisco, sus herramientas de software y los productos de hardware y software.

Este libro no trata de reinventar la rueda publicando otro glosario acerca de términos y siglas de interconectividad de redes. Cada término que se presenta en este libro se define y explica en su contexto. Pero este libro debe leerse con el navegador de Internet apuntando al sitio Web de Cisco www.cisco.com. Aunque este libro es autosuficiente, nunca está por demás buscar ayuda para reforzar algún tema recién estudiado. El sitio Web de Cisco contiene una enorme cantidad de ilustraciones, planos y otro tipo de materiales de sus productos. En particular, los lectores de este libro deben utilizar Universal Resource Locator (URL, localizador de recursos universal) para acceder a dos excelentes glosarios en línea que complementan este libro:

- **Términos y Siglas de los Sistemas de Cisco**
  www.cisco.com/univercd/cc/td/doc/cisintwk/ita/cisco12.htm
- **Términos y Siglas de la Interconectividad de Redes** www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

PARTE I

Panorama general de Cisco

CAPÍTULO 1

Cisco e Internet

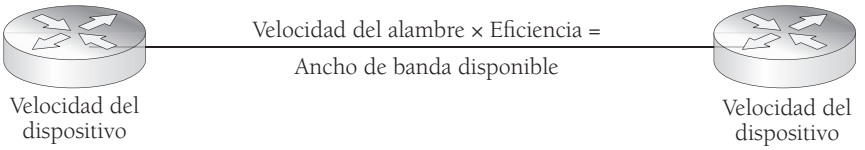
Internet es sorprendente. No existe otra palabra que describa una tecnología de la que algunos apenas habían escuchado hace 20 años, aunque en la actualidad es de uso común. La fiebre por el oro que rodea Internet hace que la carrera por el oro en California, en 1849, parezca insignificante. Sin lugar a dudas, habrá escuchado acerca de las analogías y los clichés: Internet es el mercado con el mayor crecimiento en la historia; la tecnología con el mayor crecimiento en la historia; el primer mercado realmente global de bienes, servicios e ideas. Internet ha cambiado y seguirá cambiando de manera significativa todos los sectores de la economía, desde los negocios hasta la educación y el entretenimiento. Internet es la supercarretera de la información, es nuestra vía de acceso al futuro.

INTERCONECTIVIDAD

Lo más sorprendente de todo el alboroto acera de Web es que es verdad. La mayor parte de las compañías de investigación de mercados estiman que el crecimiento de Internet será del 18% anual. De hecho, se dice que alcanzamos la marca de un mil millones de usuarios en algún momento del 2005 y se espera que se duplique esta cantidad durante la próxima década. El número de nombres de dominio registrados en Internet se duplica cada año. Existen actualmente cientos de miles de millones de páginas Web, mientras que hace 15 años sólo existía un millón de ellas. En el 2005, los publicistas gastaron una cantidad aproximada de 150 mil millones de dólares en anuncios en Internet. Cada *hora*, aproximadamente mil estadounidenses contratan el acceso a Internet. Sin importar qué tan cansados estemos de escuchar esta letanía, los números son abrumadores.

A pesar de que la mayor cobertura de la prensa se dirige a tecnologías como los navegadores y los teléfonos celulares con Internet, la verdadera acción se encuentra en la infraestructura de Internet. Miles de millones de dólares están siendo invertidos por jugadores serios que vislumbran el día en que casi todos los medios de comunicación (radio, teléfono y televisión) converjan en Internet. Esta convergencia utilizará Internet como una sola "tubería" por la que viajarán todas las comunicaciones. No existe un acuerdo acerca de si la tubería de Internet correrá a través de dispositivos inalámbricos, líneas telefónicas, cables de TV o hasta satélites. En realidad, parece ser que ocuparán todos los anteriores. Sin embargo, una gran cantidad de negocios están abriendo a diario frentes de batalla, y están invirtiendo grandes sumas de dinero en este negocio. Las apuestas son jugosas, porque ganar el juego de la infraestructura de Internet promete grandes beneficios.

Sin embargo, hay un problema en el paraíso. A medida que más gente ingresa a este mercado, se ha tenido que revisar con detenimiento el diámetro de la tubería (llamada *ancho de banda*, una medida de la cantidad de información que puede transferirse a través de un vínculo). Nuevos usuarios y aplicaciones cada vez más rápidas están consumiendo el ancho de banda con la misma rapidez con que puede agregarse nuevo equipo de red a la infraestructura de Internet (el laberinto global de los vínculos de telecomunicaciones y dispositivos de interconectividad que hace que todo funcione). Enfrentémoslo; con todos los avances, Internet aún puede ser lenta, ¿verdad? Internet sigue experimentando escasez de ancho de banda, y hay preocupación de que cargas adicionales finalmente hagan que se colapse. Lo anterior aún no ha sucedido, pero se está invirtiendo una gran cantidad de dinero y atención en la infraestructura de Internet.



Los usuarios se conectan a los servidores por medio de esta infraestructura de Internet, aunque son pocos los que saben cómo funciona. El ancho de banda no es sólo una cuestión de medios de telecomunicación que fluye por un cable de fibra óptica de alta velocidad. Los dispositivos de red instalados en cada extremo de los cables son igual de importantes. En muchas situaciones, la velocidad de estos dispositivos es un factor tan importante en el ancho de banda de Internet, como los mismos medios de telecomunicación.

En este libro se analiza la infraestructura de interconectividad desde las bases, comenzando con la tecnología, y ascendiendo hasta el nivel producto. Si usted es un principiante, lea este libro y conocerá los fundamentos de la interconectividad. Está escrito desde la perspectiva del fabricante número uno de tecnología de interconectividad, Cisco Systems. Debido a que las tecnologías se estudian genéricamente, comprenderá los sistemas y componentes que son necesarios para hacer que funcione cualquier tipo de red, no sólo una instalada con productos de Cisco. Pero no se confunda; este libro es sobre *infraestructura* (es decir, sobre los dispositivos con los que las redes trabajan):

- ▼ **Enrutadores** Estos dispositivos enrutan los datos entre redes, como redes de área local (LAN), redes de área amplia (WAN) y redes de área metropolitana (MAN). Los enrutadores ponen el *inter* en la interconectividad; sin ellos, Internet no sería factible. Los enrutadores utilizan las direcciones de protocolo de Internet (IP) para calcular cómo enrutar mejor los paquetes a través de las redes.
- ■ **Conmutadores** Estos dispositivos también envían datos en y entre LAN y han reemplazado al concentrador como el estándar *de facto* para conectar estaciones de trabajo y servidores a la red. Los conmutadores son más rápidos que los enrutadores, sin embargo, casi ninguno logra ver o utilizar las direcciones IP y, por lo tanto, no tienen la capacidad de los enrutadores para encontrar rutas entre redes más grandes. Sin embargo, hay conmutadores que incorporan el enrutamiento: se les conoce también con el nombre de "conmutadores de capa 3", y se analizarán con más detalles en páginas posteriores.
- ■ **Firewalls** Aunque pueden considerarse simples enrutadores especiales que filtran paquetes para asegurar conexiones de datos entre redes internas y externas, son dispositivos de seguridad avanzada que examinan las comunicaciones entre dispositivos en muchas capas y, después, realizan acciones específicas o determinan lo que deben dejar pasar y lo que deben bloquear.
- ▲ **Servidores de acceso** Estos dispositivos dedicados responden llamadas telefónicas desde usuarios remotos y los conectan a la red. Casi todos los servidores de acceso son utilizados por los proveedores de servicios de Internet (ISP) para conectar usuarios domésticos y pequeños negocios a Internet.

De manera colectiva, estos dispositivos conforman la infraestructura de Internet. El único ingrediente principal adicional son los vínculos de telecomunicaciones que se usan para realizar las conexiones WAN. En este libro, estudiaremos cada tipo de dispositivo, de acuerdo con la línea de productos de Cisco, y revisaremos también las tecnologías WAN. Al hacerlo así (desde la perspectiva de la línea de productos de Cisco) se proporcionará una idea más detallada de lo que pasa dentro de los dispositivos de interconectividad.

La posición de Cisco en la industria de la computación

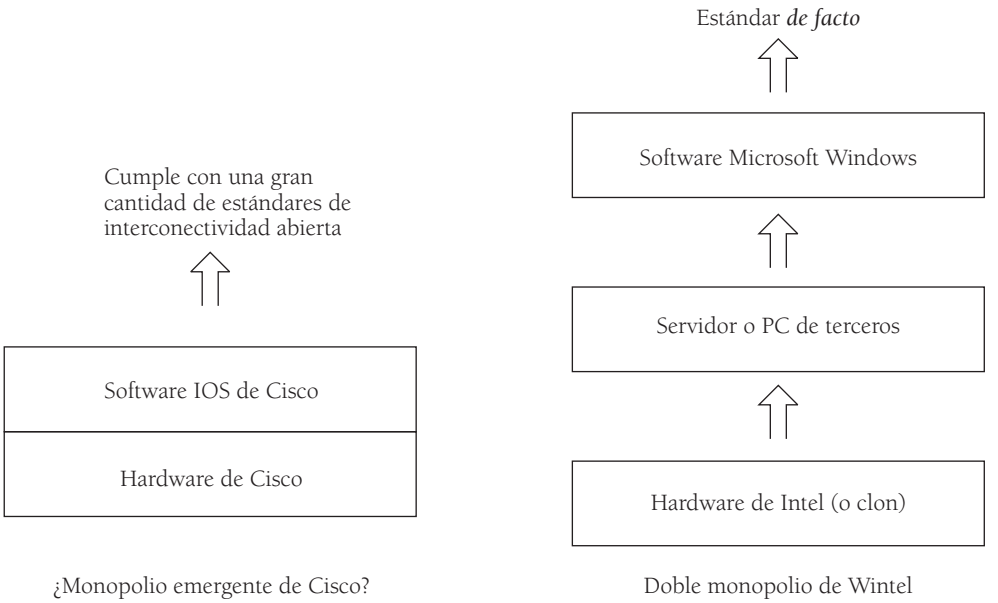
Todos sabemos que Microsoft Windows es, en la actualidad, el sistema operativo para computadoras más popular. Sin embargo, aquí le presentamos un examen de opción múltiple: ¿Puede usted nombrar el segundo sistema operativo más importante? Seleccione uno:

- ▼ **MVS** Es el sistema operativo de propietario de IBM utilizado en computadoras grandes. MVS aún tiene acaparados los centros de datos corporativos y gubernamentales que manejan la contabilidad financiera y otras transacciones importantes.
- ■ **UNIX/LINUX** En realidad, existen cerca de una docena de versiones de propietario de UNIX, de fabricantes de computadoras como Sun, HP, Compaq, Novell e IBM. LINUX, el "nuevo" vecino de la calle, ha adquirido gran popularidad. Sin embargo, el "viejo y buen" UNIX aún es el sistema operativo más dominante para servidores en aplicaciones cliente-servidor de clase empresarial.
- ▲ **IOS** Son las siglas de Internetwork Operating System; se trata del sistema operativo propietario de Cisco Systems para su línea de hardware de interconectividad.

Puesto que éste es un libro de Cisco, se trata de una pregunta con intención. IOS es el segundo sistema operativo más importante, y por un gran margen de diferencia. Hasta cierto punto aseguramos lo anterior porque UNIX y MVS han perdido su delantera (UNIX ha perdido mercado ante Microsoft Windows y MVS y, aunque aún es una tecnología de tarea crítica, ha dejado de crecer). Sin embargo, la razón principal de que IOS sea tan importante es que Cisco tiene más del 80% del mercado de enrutadores de Internet, e Internet es el mercado con el más rápido y mayor crecimiento en la historia.

Para poner lo anterior en perspectiva, Cisco tiene casi la misma participación en el mercado en la tecnología de enrutadores que Intel en plataformas de hardware Windows, o *Wintel*. El régimen de Wintel ha sido atacado como monopolio por sus competidores y el Departamento de Justicia de Estados Unidos. No pasa lo mismo con Cisco. IOS es su arquitectura propietaria de sistema operativo y opera solamente en su hardware. Esto significa que el liderazgo en el mercado de Cisco obtiene ganancias del hardware y el software, y proporciona a la compañía control arquitectónico total sobre sus productos.

La posición actual de Cisco tiene sus fortalezas y debilidades comparadas con el doble monopolio de Wintel. Por el lado negativo, los productos de Cisco son muy utilizados para ejecutar protocolos de estándares abiertos, lo que reduce el alcance al que pueden impulsar la arquitectura del producto para tomar el control del mercado. Cisco no congela totalmente a ningún competidor de los ciclos de diseño para preparar productos que implantan tecnologías emergentes, porque las tecnologías implantan estándares abiertos. Por el lado positivo, Cisco es una compañía particular que hace sus propios productos. Esto contrasta



favorablemente con Wintel, un par de compañías que dependen de cientos de fabricantes de PC para entregar sus respectivos productos a un mercado altamente fragmentado.

Desde el punto de vista financiero, al terminar el milenio, Cisco permaneció inadvertida. A pesar de que podía mencionar el nombre de la compañía a ciertas personas que no podrían diferenciar entre Cisco y Crisco, es muy probable que alguna parte de sus vidas estuviera en contacto con algún producto de la compañía. Quizás la red de computadoras en su trabajo utilizaba equipo de Cisco; quizás el ISP que contrataban para conectarse a Internet utilizaba equipo Cisco. Pero lo importante del asunto es que en un punto en la historia, Cisco fue la compañía más valiosa en la faz de la tierra. En marzo del 2000, menos de dos décadas después de que se fundó la compañía, ésta alcanzó un valor de 500 mil millones de dólares.

Sin embargo, más de un año después, todo cambió. Cuando apareció la ráfaga de las compañías dot.com, Cisco decayó. Muchas compañías ya no dependieron del equipo de Cisco y para la primavera del 2001, Cisco enfrentó una anulación de deuda de dos mil millones de dólares. De su posición como líder, con acciones de 146 dólares cada una en marzo del 2000, éstas bajaron a un poco más de ocho dólares en octubre de 2002. A pesar de que Cisco se vino abajo, no decayó tanto como otras compañías que tuvieron que cerrar operaciones. Cisco se ha mantenido ahí y se ha levantado de manera constante. A principios del 2006, las acciones de Cisco se vendían a 20 dólares cada una y las ganancias del segundo trimestre alcanzaron seis mil 600 millones de dólares. ¿Cuál fue el resultado de esta lección en finanzas? Cisco cayó, pero no salió del mercado.

Sin embargo, este libro no es para ensalzar a Cisco. Como cualquier otra industria, esta compañía tiene sus fallas y en estas páginas se le criticará fuertemente cuando se requiera. Pero si usted es una persona que planea hacer carrera o un gerente que diseña la estrategia de Internet de su compañía, aprender cómo funciona la tecnología de Cisco es la mejor forma de entrar al mundo de la interconectividad.

El panorama de Internet

Internet no es una sola tecnología: es una colección de tecnologías relacionadas que hacen posible la conectividad.

- ▼ **Medio físico** Los vínculos físicos que conectan a los equipos son la base del trabajo en red, desde los conectores hasta los cables de fibra óptica de alta velocidad.
- ■ **Tecnologías de red** Los protocolos LAN regulan lo que sucede en el cable. El más conocido es Ethernet, pero existen otros muy importantes.
- ■ **TCP/IP** El protocolo de control para la transmisión/protocolo Internet es lo que conecta a Internet. IP maneja el direccionamiento y TCP la mensajería. Dentro del conjunto de protocolos de Internet también se incluye el protocolo de datagrama de usuario (UDP), que se utiliza para enviar datagramas más rápidamente y a tiempo en una red. El protocolo de mensajería de control de Internet (ICMP) es otro componente que se utiliza para enviar mensajes de error en una red.
- ■ **Tecnologías operativas** Las redes dependen de un gran número de estándares y protocolos para operar por sí mismos, sin los cuales la conectividad no sería práctica.
- ▲ **Protocolos de aplicación** Las aplicaciones de red definen los tipos de tareas que las conexiones pueden hacer, desde las transferencias de archivos hasta las descargas de páginas Web.

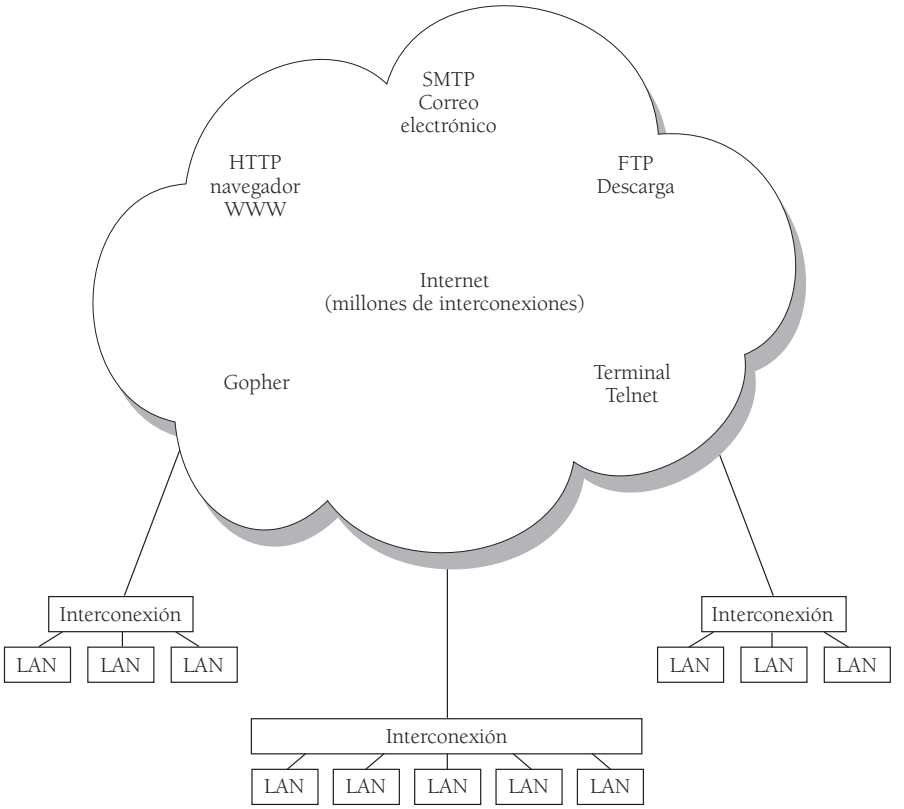
Para diseñar sus productos, la industria de la conectividad utiliza un modelo arquitectónico de siete capas llamado modelo de referencia para la interconexión de sistemas abiertos (OSI). No es una coincidencia que la lista anterior de tecnologías se adhiera más o menos al modelo OSI, desde el nivel físico hasta el más alto.

Antes de seguir adelante, unas pocas palabras para asegurarnos que nuestra terminología es clara: *Internet* es una interconexión global de redes individuales. Una *interconexión* puede ser cualquier colección de redes de área local (LAN) que funcionan bajo el mismo régimen administrativo (por lo general una compañía o un proveedor del servicio de Internet). Una interconexión privada es, desde el punto de vista mecánico, lo mismo que la Internet abierta. Un *host* es un dispositivo de usuario, como una PC, un servidor, un mainframe o una impresora. Un *dispositivo* es un equipo de red, como un enrutador. Los términos genéricos *nodo* y *estación* se refieren tanto a hosts como a dispositivos. Un *segmento LAN* es un medio de red que hospeda un recurso compartido. Un *protocolo de aplicación* es un software estándar que hace que funcionen cosas como navegadores Web, transferencias de archivos, correos electrónicos y otras funciones útiles. Una *intranet* es una red interna que funciona como una Web privada que cuenta con software para aplicaciones corporativas utilizadas mediante navegadores Web en lugar de interfaces gráficas de usuario (GUI) más tradicionales, como Microsoft Windows.

Desde el punto de vista técnico, las interconexiones privadas están conformadas de las mismas partes que Internet. Lo único que las distingue a Internet de una interconexión grande es su alcance.

Cuatro tipos principales de dispositivos de interconectividad

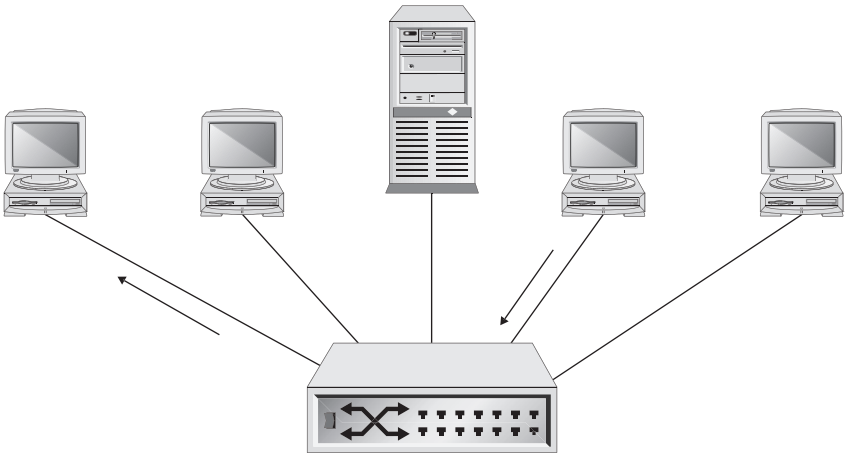
Un *conmutador* conecta hosts a la interconexión, de la misma forma que un concentrador. Sin embargo, los conmutadores son diferentes, en el sentido de que forman un circuito virtual



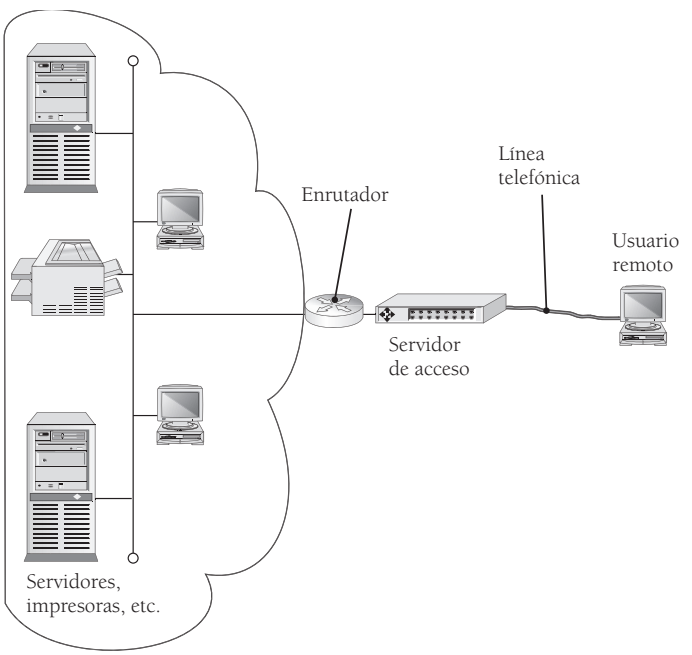
entre los hosts emisor y receptor. En otras palabras, el ancho de banda del conmutador está reservado para una sola conexión conmutada entre dos hosts, como si estuviera 100% dedicado a ese circuito virtual. Los conmutadores pueden hacer esto utilizando equipo electrónico de mejor calidad que el que utilizan los concentradores para dividir el ancho de banda en fragmentos (llamados *canales*) lo suficientemente grandes para brindar servicio a cada puerto del conmutador. Los conmutadores cuentan con casi todo, excepto con los concentradores reemplazados.

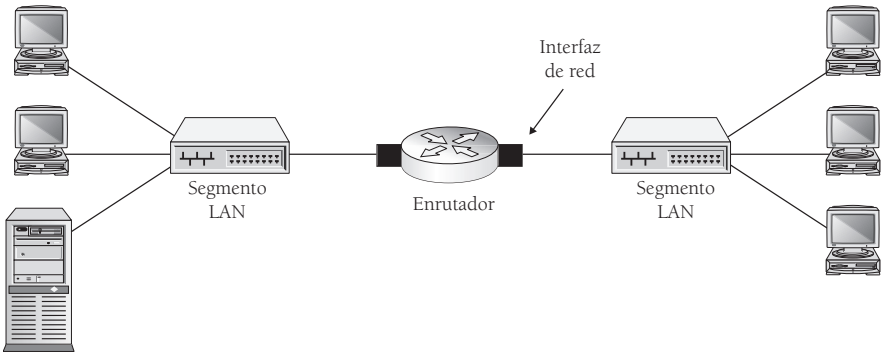
Un *servidor de acceso* es un dispositivo especializado que, en palabras muy burdas, funciona como un módem en un extremo y como un concentrador en el otro. Los servidores de acceso conectan usuarios remotos a las interconexiones. La mayor parte de los millones de puertos de servidores de acceso que existen en el mundo son administrados por ISP para que tomen llamadas telefónicas de suscriptores de Internet. Algunos llevan a cabo funciones más especializadas, pero el propósito principal del servidor de acceso es conectar usuarios por marcación remota a una interconexión. Estos servidores a menudo proporcionan conectividad analógica a una red.

Un *enrutador* es un dispositivo inteligente que reenvía el tráfico con base en la dirección IP de un mensaje. Mientras que los conmutadores cuentan con puertos a los que se conectan hosts individuales, los enrutadores tienen interfaces a las que se conectan los segmentos de una LAN. En términos más simples, el trabajo de un enrutador es transferir *paquetes* de datos entre los segmentos LAN conectados.



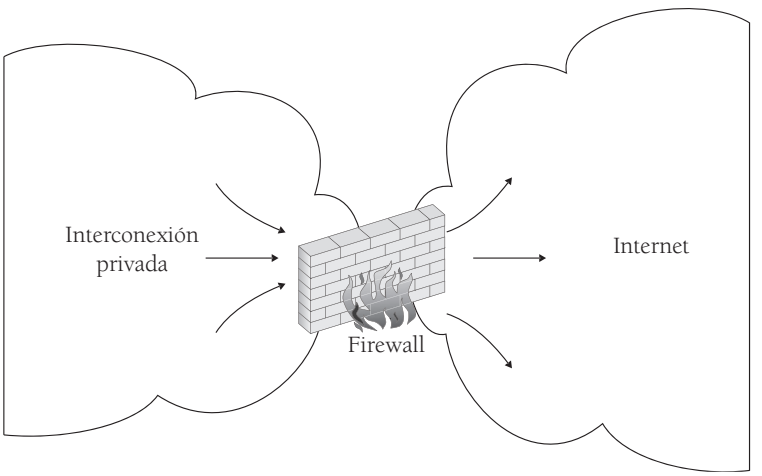
El enrutador es el tipo de dispositivo más importante en la interconectividad. Proporciona la flexibilidad y el poder de decisión que hace posible la operación de complicadas interconexiones. Sin la capacidad lógica que brindan los enrutadores, Internet sería cientos de veces más lenta y más cara. Como se explicará de manera detallada en el capítulo siguiente, las arquitecturas de interconexión tienen siete capas: los conmutadores operan de manera predominante en la capa 2 y los enrutadores en la capa 3. Los enrutadores también cuentan con la capacidad de filtrar tráfico con base en las direcciones de origen y de destino, en la aplicación de red y otros parámetros.





Los *firewalls* son dispositivos de red que actúan como puntos de verificación entre una interconexión y el exterior, filtrando paquetes que no pertenezcan a la red. Su tarea es verificar que cada paquete cumpla con las políticas de seguridad con las que han sido programados. Un firewall forma un punto de estrangulamiento intencional de tráfico y, continuamente supervisa que las conexiones internas/externas cumplan con las reglas de seguridad. Cualquier compañía conectada a Internet debe tener un firewall configurado.

Los firewalls más potentes tienen hardware especializado, pero esto no siempre es necesario. Un enrutador normal puede programarse para llevar a cabo muchas tareas de un firewall, aunque en casi todos los casos, se prefiere un dispositivo firewall dedicado. Los firewalls se usan internamente cada vez más para salvaguardar activos de posibles amenazas internas.



Topologías básicas de interconexión

Una *topología* es la disposición física de los nodos en una interconexión. En general, una topología se expresa como un mapa lógico que representa gráficamente cada uno de los nodos y los vínculos físicos que los conectan. En realidad, los mapas topológicos se utilizan como la GUI a través del cual funcionan casi todas las herramientas de software de administración. En la figura 1-1 se muestran los elementos básicos de red que se combinan de una manera u otra para formar las interconexiones.

El segmento LAN es la parte fundamental con que se construyen las interconexiones. Dicho de otra forma, los segmentos LAN son las unidades de red que vinculan a las interconexiones. Internet es una colección de millones de segmentos LAN. La razón por la que usamos el término formal *segmento* LAN es que las colecciones locales de segmentos individuales se conocen comúnmente como "LAN" a pesar de que, estrictamente hablando, son en realidad interconexiones locales. Lo anterior parece quisquilloso, pero se sentirá a gusto con esta distinción en capítulos posteriores.

Las conexiones remotas utilizan circuitos telefónicos, cables y señales por satélite para enlazar hosts desinstalados físicamente en el segmento LAN. El enlace de telecomunicaciones puede ser de cualquier tipo, desde una línea analógica normal de voz, hasta una línea de suscriptor digital (DSL), de banda ancha, basada en cable y hasta de banda ancha satelital; todas ellas son tecnologías que en la actualidad resultan comunes para usuarios de una pequeña oficina o una oficina casera.

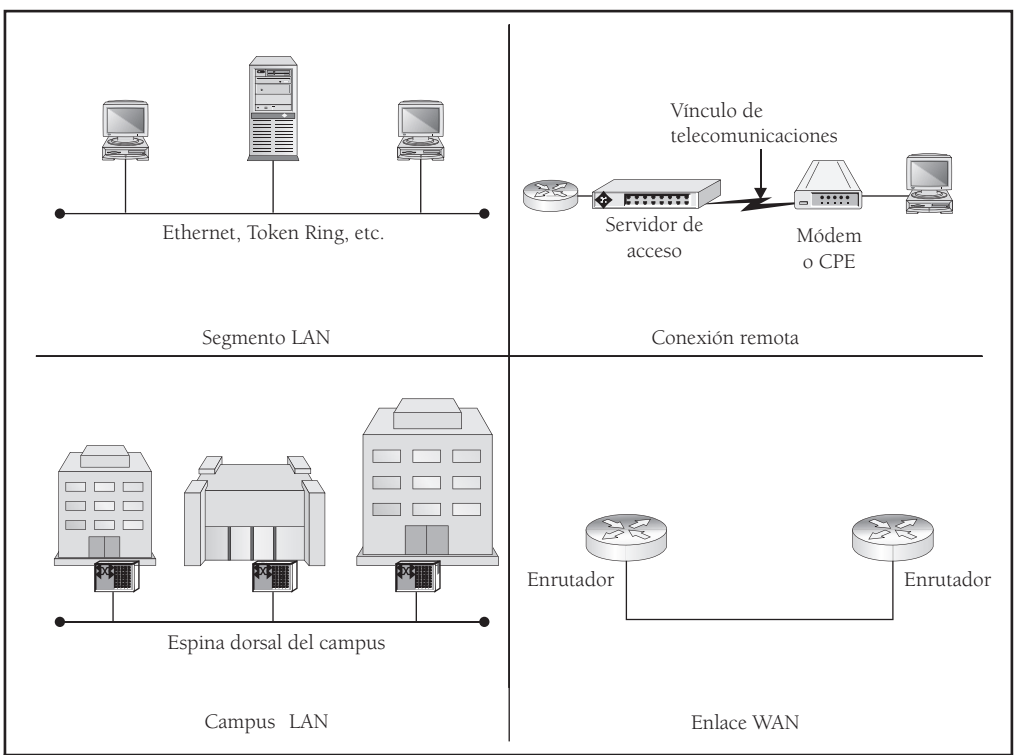


Figura 1-1. Existen cuatro elementos básicos de topologías de interconexión.

LAN de campus es un nombre inapropiado pero acostúmbrese a él. Cisco lo utiliza como término genérico para describir interconexiones locales corporativas. La mayoría están instaladas en un solo edificio y no a lo largo de todo un campus de oficinas, además de que todas están formadas por múltiples segmentos LAN, no por una sola LAN. Sin embargo, las LAN instaladas en campus se distinguen por el uso de un segmento de espina dorsal de alta velocidad para interconectar los demás segmentos LAN locales. La mayoría de las espinas dorsales de LAN "de trabajo pesado" operan a través de cableado de fibra óptica.

Los vínculos WAN (red de área amplia) son vínculos de telecomunicaciones entre ciudades, aunque algunos se encuentran instalados en el fondo de los océanos para conectar continentes. Casi todos los nuevos vínculos WAN que se están instalando usan fibra óptica de ultra alta velocidad. Lo más actual aún se considera el OC-768, con una velocidad de transferencia de datos de 40 Gbps. (OC quiere decir *optical carrier*, transportador óptico; Gbps quiere decir *gigabits por segundo.*) Los vínculos WAN de menor velocidad funcionan sobre tecnologías de las cuales quizás haya escuchado algo: T1 y T3 (también llamada DS3), que funciona a 1.5 Mbps y 45 Mbps, respectivamente.

Jugadores en el mundo de la interconectividad

No existe una "red de Internet" como tal. En otras palabras, no existe una red dedicada, troncal e independiente que sea operada bajo los auspicios de alguna autoridad administrativa central. En realidad, Internet es una colección de redes individuales sin costo unida por dos cosas:

- ▼ **Tecnologías que permiten el intercambio** Grupo de estándares y tecnologías *de facto* que no sólo hacen factible la conectividad individual, sino que también permiten que las interconexiones interactúen automáticamente con otras interconexiones.
- ▲ **Protocolo de Internet (IP)** Sistema de comunicaciones aceptado globalmente que posibilita la conexión y el intercambio de datos con hosts que no sean compatibles en cualquier lugar del mundo. IP unifica la comunicación entre casi todos los sistemas de cómputo en un sistema de direccionamiento y de formato unificado de datos.

En la figura 1-2 se muestra de manera aproximada cómo se forma Internet. El prerrequisito es que los usuarios necesitan estar en una red de algún tipo, y en estos días, en una oficina o planta industrial, esto suele significar algún tipo de LAN Ethernet. En el pasado, los protocolos de escritorio, como Novell NetWare IPX y AppleTalk, utilizaban sus respectivos protocolos en Ethernet. En la actualidad, casi todas las computadoras de escritorio y las redes a las que éstas se encuentran conectadas, utilizan el protocolo TCP/IP sobre Ethernet.

Los ISP juegan un papel primordial en la conectividad de Internet para empresas, no solamente para usuarios domésticos. La conectividad de igual a igual es la forma como se intercambia el tráfico entre los diferentes ISP. Desde el punto de vista de Internet, la unión clave es donde usted se conecta a la red de igual a igual (un grupo de miles de enrutadores de alta velocidad que transfieren rutas y tráfico IP entre sí). A pesar de que algunas empresas muy grandes (grandes corporaciones, agencias gubernamentales y universidades) tienen sus propias conexiones directas a la red de igual a igual, casi todos se conectan a través de los ISP.

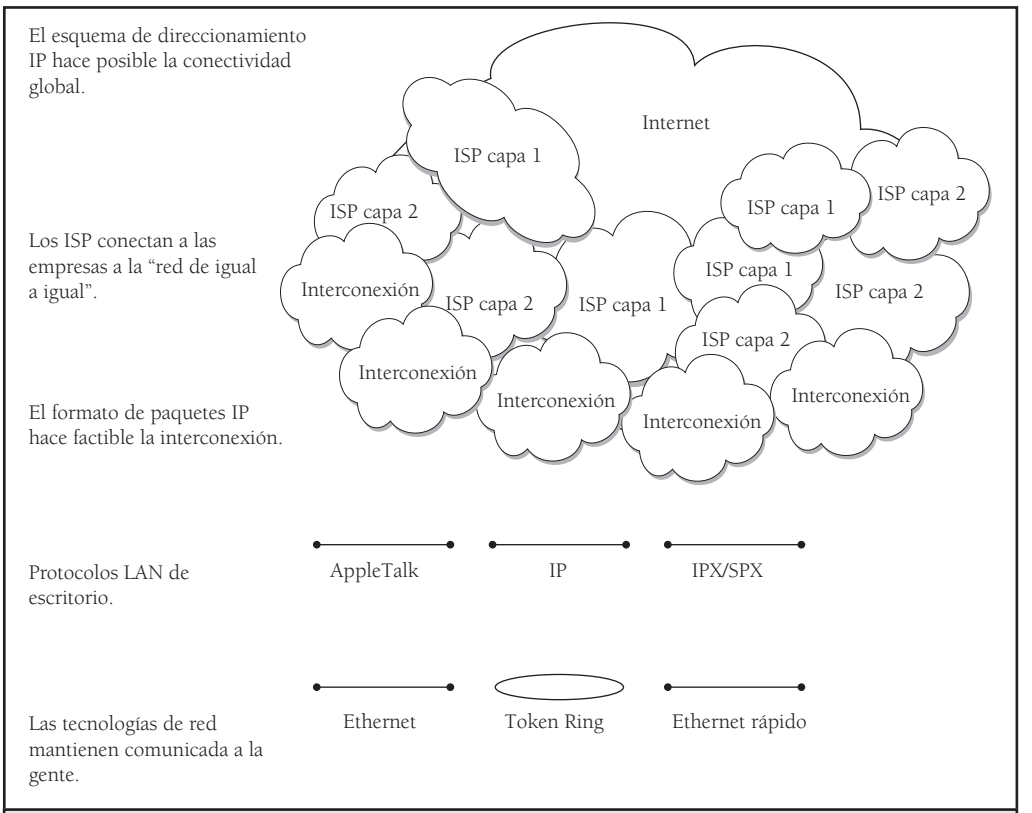


Figura 1-2. Internet global es un conjunto por capas de diferentes sistemas independientes.

El ingreso a la red de igual a igual casi siempre se lleva a cabo mediante una línea troncal de fibra óptica de alta velocidad, controlada generalmente por los llamados proveedores de espina dorsal de Internet (IBP), como AT&T, MCI y AOL. A estos IBP también se les conoce como proveedores de servicio de Internet capa 1. Se conectan "viéndose" entre sí. De *igual a igual* es un conjunto de conexiones acordadas que los ISP tienen entre sí para el intercambio del tráfico de la red. Estas conexiones suelen ser de ultra alta velocidad (fibra OC 198, etc.), se realizan en muchos lugares alrededor del mundo y se conocen con el nombre de puntos de conexión de igual a igual.

Los proveedores de capa 2 representan el nivel siguiente. Éstos no ven directamente a la espina dorsal; en cambio, compran el acceso de los portadores de capa 1 y después lo revenden a negocios, consumidores y otros prestadores de servicios. Casi todos los negocios y los consumidores en general contratan su conectividad a Internet por medio de un portador de capa 2 o de un proveedor de servicios que revende el acceso.

Protocolos de interconexión

Los protocolos son la clave de la interconectividad. Un *protocolo* de red es un formato de datos establecido y un conjunto de reglas para el intercambio de mensajes que gobierna

Capa 3	IP	Interconectividad
Capa 2	Ethernet, Token Ring, etc.	Acceso al segmento LAN

un proceso específico. Los dos protocolos más fundamentales de Internet se encuentran en las capas inferiores del modelo OSI. Son los diversos protocolos de red (o LAN) y el protocolo IP.

Este libro se concentra principalmente en las capas 2 y 3, porque ahí es donde Cisco y sus competidores dan vida a la infraestructura de red física como interconexiones. La capa 2 conecta el host a su segmento LAN doméstico y la capa 3 interconecta los segmentos LAN. (En caso de que se lo pregunte, la capa 1 abarca el cableado y otros medios de transporte físicos.)

Sin embargo, ese es sólo el comienzo de la historia de los protocolos. Existen literalmente docenas de protocolos suplementarios, grandes y pequeños, para llevar a cabo cualquier tarea, desde verificar si el dispositivo vecino aún está funcionando hasta calcular la mejor ruta para el envío de paquetes al otro lado del mundo.

Por ejemplo, considere el protocolo de inicio de sesión (SIP). El SIP es un estándar de la Internet Engineering Task Force (IETF) (RFC 3261) que administra la manera en que pueden existir la voz, el video y los datos en la misma red. Con mucha frecuencia, verá al SIP como en tecnologías y dispositivos de Voz sobre IP (VoIP). Debido a este protocolo, VoIP puede utilizarse en computadoras de escritorio, asistentes digitales personales (PDA), teléfonos IP y otros dispositivos.

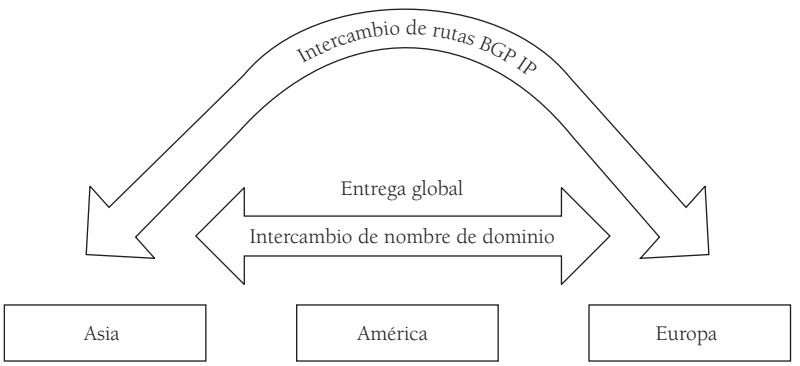
Estos protocolos complementarios pueden dividirse en tres grupos: mantenimiento, administración y enrutamiento.

Protocolos de enrutamiento.	Rutas óptimas.	Intercambian actualizaciones, calculan las rutas óptimas.
Protocolos de administración.	Salud y seguridad.	Monitorean el desempeño, hacen sonar las alarmas, reconfiguran.
Protocolos de mantenimiento.	Limpieza.	Descubren dispositivos, trazan rutas, notifican a los vecinos.

Cuanto más cerca se encuentren los protocolos de red del hardware de dispositivo de red, tenderán a ser más de propietario (específicos de un proveedor). Por ejemplo, el protocolo

de descubrimiento de Cisco da seguimiento a los dispositivos (pero sólo a los de Cisco). Los protocolos de administración son más genéricos. Sin embargo, Cisco es tan grande que dichos protocolos soportan los protocolos estándares de la industria, además de promover su propio protocolo de seguridad. Un tercer tipo de protocolos de mantenimiento, llamados protocolo de enrutamiento, son los que hacen posible las grandes y complejas redes.

Los protocolos de enrutamiento se encargan de gran parte del trabajo y la complejidad en redes muy grandes al rastrear automáticamente las rutas que se utilizarán entre direcciones IP. El protocolo de gateway fronteriza (BGP) es el protocolo de enrutamiento de alto nivel que conecta todo dentro de las ciudades, entre éstas y entre continentes. Existen otros protocolos de enrutamiento que se utilizan para mantener un registro de las rutas dentro de las interconexiones privadas. Cisco soporta los protocolos de enrutamiento estandarizados en la industria, además de promover un par de protocolos propios de enrutamiento interno por sí mismo.



Comparación entre enrutamiento y conmutación

Hace algunos años, se inició una guerra tecnológica entre el enrutamiento y la conmutación. Es probable que hayan pisoteado a los concentradores hasta extinguirlos, pero ni la conmutación ni el enrutamiento pudo declarar la victoria. A medida que los dispositivos se abarataron y se hicieron más potentes, los conmutadores surgieron como una alternativa viable para los concentradores en el extremo inferior y los enrutadores en el extremo superior. Debido a que los conmutadores son inherentemente más rápidos, hubo presión para reemplazar las redes enrutadas por conmutadas. La batalla se llevó a cabo en ambos extremos del terreno de la interconectividad. En el extremo inferior (llamado *capa de acceso*, porque allí es donde los hosts obtienen el acceso a la interconexión), los conmutadores han reemplazado a los concentradores como dispositivo predilecto para conectar hosts, debido al gran ancho de banda de los conmutadores. Éstos han desplazado también a los enrutadores como espina dorsal que conecta a las LAN dentro de un edificio o campus. Los conmutadores de capa 3 pueden llevar a cabo las tareas normales de enrutamiento. En la figura 1-3 se muestran los tres diferentes tipos de conmutadores.

La conmutación ha sido siempre la norma en las WAN troncales, como los vínculos de fibra óptica que los proveedores de Internet operan entre ciudades. En realidad, los sistemas

telefónicos de voz son redes conmutadas construidas sobre circuitos físicos permanentes en forma de cables telefónicos instalados en los negocios y las casas.

Desde luego, los conmutadores de datos no cuentan con cableado (los circuitos de conmutadores que crean son virtuales). Es decir, los conmutadores crean circuitos lógicos (no cableados) temporales de extremo a extremo, que se establecen y se eliminan conforme a las necesidades. Sin embargo, los conmutadores de datos son inherentemente más rápidos que las redes compartidas. La frase "conmuta cuando puedas, enruta cuando debas" se ha convertido en el lema de la industria (lo que significa es que siempre que sea posible, debe utilizar conmutadores de acceso en lugar de concentradores para el acceso al host y conmutadores LAN en lugar de enrutadores para interconexiones).

Revise cuidadosamente la figura 1-3 y observe que las dos tecnologías tienen sus respectivas ventajas y desventajas. En pocas palabras, los enrutadores son más lentos y costosos, pero más inteligentes. De hecho, las redes de gran tamaño nunca podrán operar sin algún tipo de funciones de enrutamiento. Por lo tanto, la industria está experimentando la mezcla de la velocidad de capa física de la conmutación y la inteligencia de la capa de red del enrutamiento. Se han creado dispositivos híbridos que incorporan parte de la inteligencia de enrutamiento IP en el hardware. Estos híbridos han recibido el nombre de conmutadores de capa 3, conmutadores multicapa, etcétera.

Otras tendencias en interconectividad

Más allá de la guerra tecnológica del enrutamiento contra la conmutación, un gran número de tendencias están en proyecto en la industria de la interconectividad:

- **Administración de red** Se ha sostenido gran presión para hacer más confiables y administrables las interconexiones grandes y complicadas. Las empresas están adoptando el llamado software de consola de administración o de estación de administración de red (NMS), que permita a su personal de redes supervisar y reparar fallas de sus interconexiones de manera centralizada. Estas consolas NMS están siendo operadas mediante un par de protocolos de administración de red establecidos pero aún en desarrollo.
- **Seguridad de red** Hasta la fecha, casi todos los esfuerzos de la industria se han concentrado en el acceso seguro a los paquetes de la red. Ahora la tendencia está cambiando hacia el cifrado de sus contenidos para garantizar virtualmente la seguridad y la integridad de los datos. Una estricta seguridad requiere de un equilibrio entre gasto, desempeño o ambos.
- **Redes privadas virtuales (VPN)** Los vínculos VPN están desplazando rápidamente a los vínculos WAN tradicionales de líneas arrendadas. Las VPN utilizan cifrado para permitir que los corporativos operen WAN privadas por medio de Internet (a una fracción del costo). De nuevo, el cifrado tiene un costo en rendimiento. También se plantean problemas de confiabilidad que a menudo hay que resolver.
- **Vínculos más rápidos de marcación** La tecnología de acceso remoto mediante marcado telefónico para casas o pequeñas oficinas está siendo actualizada al reemplazar los circuitos de línea telefónica convencionales con circuitos digitales. En cierto momento, la red digital de servicios integrados (ISDN) parecía la respuesta,

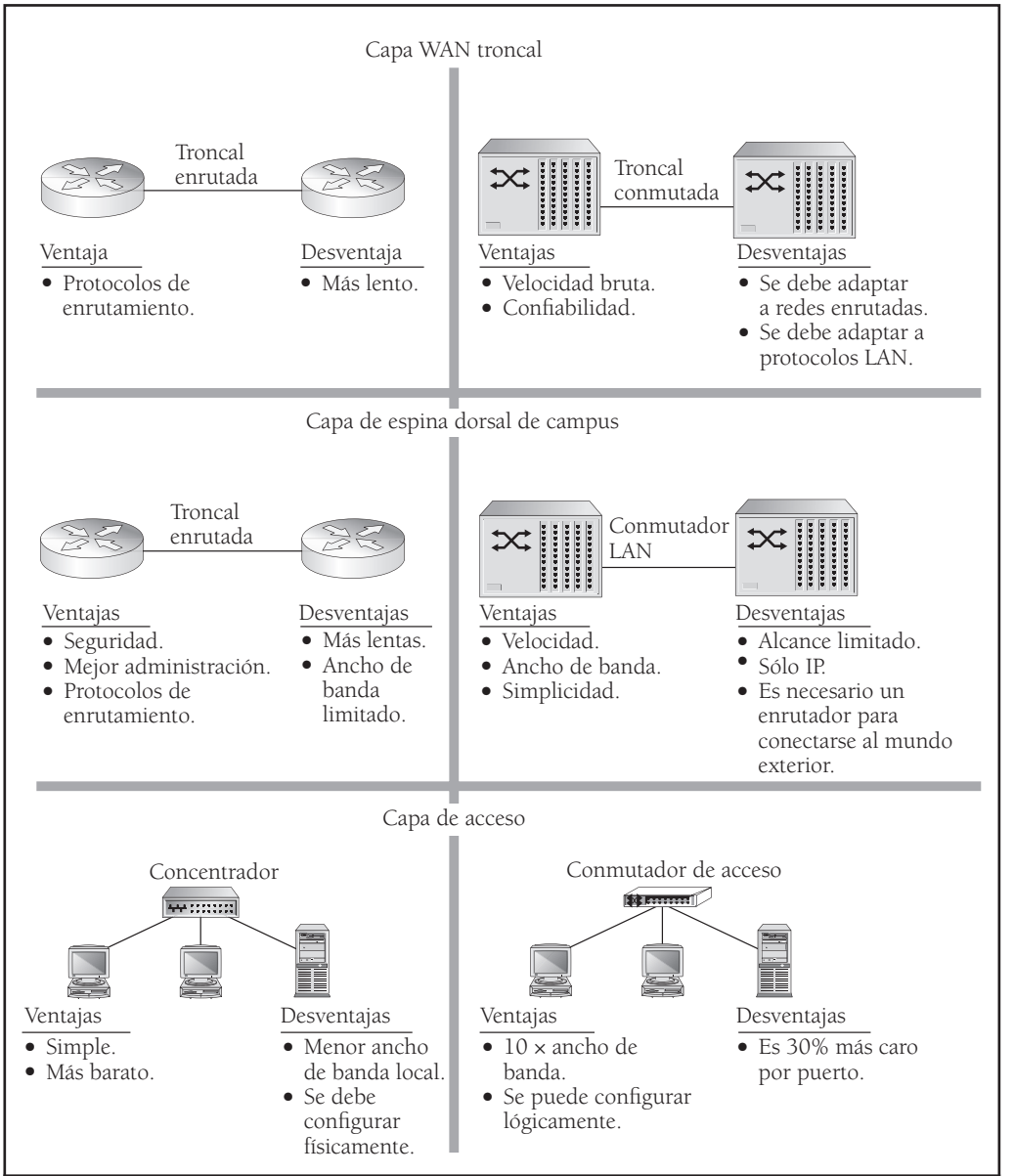


Figura 1-3. Los conmutadores están invadiendo el terreno de los concentradores en el extremo inferior y los enrutadores en el extremo superior.

pero ahora el DSL y el cable son vistos como la forma más probable de recorrer la "última milla" desde la central telefónica de la compañía de teléfonos hasta la casa o pequeña oficina.

- **WAN troncales más rápidas** Las líneas troncales que funcionan bajo el estándar red óptica sincrónica (SONET) están avanzando a pasos agigantados. El OC-1 a 52 Mbps original ha sido mejorado paulatinamente hasta el estándar actual OC-768 a 40 Gbps.
- **Tecnologías de espina dorsal** El mercado de espina dorsal de campus tiene dos protocolos de red de gran ancho de banda: el modo de transferencia asincrónica (ATM) y el Gigabit Ethernet. ATM es un estándar no IP a 622 Mbps, ideal para tráfico multimedia, que tiene la característica de garantizar calidad de servicio. Sin embargo, debe adaptarse para su uso en redes Ethernet. Como su nombre lo implica, Gigabit Ethernet es el sucesor a 1 000 Mbps de la especificación Fast Ethernet a 100 Mbps.
- **Telefonía IP** Por años, las líneas telefónicas convencionales se han usado para facilitar las conexiones WAN o hasta al usuario casero o de pequeña oficina, al llamar a un ISP para ingresar a la red. Sin embargo, la calle es de doble sentido. Gracias a la telefonía IP, las redes de computadoras pueden utilizarse para transportar llamadas de voz. En esencia, las llamadas se convierten al protocolo Internet (IP) y los paquetes se envían por la red a su destino, donde son convertidos de nuevo en ondas sonoras. Un beneficio importante de la telefonía IP es el ahorro en costos (con una red de datos ya instalada, es sólo cosa de agregar un sistema telefónico IP). La telefonía IP no es nada nuevo: así es como las compañías telefónicas envían las llamadas entre centrales telefónicas regionales.
- **Inalámbrico** Las redes de computadoras convencionales habían tenido un obstáculo muy importante: los equipos tenían que conectar a conmutadores y concentradores con cableado de categoría 5. Evidentemente, esta situación no es la ideal en ambientes donde las computadoras y la movilidad deben interactuar. La solución es la tecnología inalámbrica, que permite que las computadoras estén conectadas a la red sin tener que estar atadas a un cable. En meses recientes, la tecnología inalámbrica ha dado pasos agigantados, permitiendo la conectividad sin cables a velocidades cada vez mayores.
- **Multimedia** Hace seis años, disfrutar del video y escuchar música en las computadoras era sólo un sueño. Las personas que contaban con conexiones de banda ancha lo podían hacer, pero nadie más. Sin embargo, a medida que ha aumentado la popularidad de las conexiones de banda ancha, hay más contenido multimedia en Internet. Como tal, existe la necesidad de una manera eficiente de proporcionar a la gente el contenido que desee.
- ▲ **MPLS** Suele considerarse a los conmutadores de etiquetas de multiprotocolo (MPLS) como un componente clave de la "red IP de la próxima generación". Desde la perspectiva de las redes, MPLS es una tecnología de reenvío de paquetes y de conmutación. MPLS se puede interconectar con IP, ATM, Frame Relay y otros protocolos, haciéndolo muy útil para las redes de área amplia (WAN) y otras redes. MPLS se diseñó para proporcionar velocidad y escalabilidad y soporta una calidad de servicio (QoS) robusta.

Estas tecnologías y estándares tienen satisfechos a todos los proveedores de la industria de la conectividad. Los competidores más pequeños han tendido a concentrarse en un nicho en particular y seleccionan una tecnología, apostando a que prevalecerá sobre las demás. Los competidores grandes tienen más recursos y tienden a ser más pragmáticos; esto es particularmente cierto en el caso de Cisco.

PRODUCTOS DE CISCO

Cisco Systems cuenta con la línea de productos más amplia y extensa en el mercado de la interconectividad. Quedará sorprendido la primera vez que tenga en sus manos el catálogo de productos (tan grueso y pesado que recuerda a los catálogos de una gran compañía de computadoras como IBM o Hewlett-Packard).

La línea de productos ha estado en constante cambio desde hace algunos años. Esto se ha debido parcialmente a la incansable introducción en la industria de nuevas tecnologías y estándares, causando así un cambio continuo en la línea de productos. Sin embargo, dicho cambio tiene mucho que ver con la búsqueda constante de Cisco por adquirir tecnología.

La línea de productos de Cisco se divide en dos categorías:

- ▼ **Dispositivos** Productos específicos de hardware descritos al comienzo de este capítulo.
- ▲ **Soluciones** La combinación de hardware, software y servicios para satisfacer ciertas necesidades de los clientes.

La parte relacionada con las soluciones en la industria se relaciona un poco con la moda, pero es un buen indicio de dónde y cómo Cisco vislumbra a sus productos individuales en la práctica. Por ejemplo, ahora se tiene un enfoque estratégico en la Voz sobre IP (VoIP). Si se convierte en una realidad la tan sonada convergencia de datos/voz, existe la probabilidad de que Cisco, como fabricante número uno de dispositivos IP, se convierta en un fabricante clave de equipo para su utilización en compañías telefónicas y hasta de teléfonos de datos para oficina.

Competencia

Como ya se mencionó, la característica principal de la línea de productos de Cisco es que la mayoría de los productos trabajan bajo el sistema operativo de conectividad (IOS). Cisco le mencionará que lo anterior permite que los clientes lleven a cabo un mejor trabajo de configuración y administración de redes. La competencia le mencionará que el IOS hace que los dispositivos sean más costosos y que niega la posibilidad de que el cliente tome decisiones relacionadas con la tecnología en un futuro. Ambas posturas son correctas, por supuesto (todo tiene sus pros y sus contras).

A pesar de que Cisco está bien resguardado en la batalla de los productos de interconectividad, existen otras compañías que se esfuerzan por entrar en la batalla, con el deseo de ganar el suficiente terreno para hacerse un nombre en la industria.

Pisándole los talones

Cisco no es a prueba de balas. La compañía se ha dado cuenta de que hay compañías ambiciosas que quieren comerle el mandado. Existe un gran número de ejemplos que muestran en qué áreas la competencia está ganando terreno en la carrera de los proveedores de servicios para la interconectividad. Los desafiantes más poderosos son Juniper Networks en el campo de los enrutadores de alta velocidad para Internet, Nortel Networks en el campo de los equipos para redes ópticas y Redback Networks en el campo de los conmutadores.

Una de las razones principales por las que Cisco está perdiendo terreno en la venta a proveedores de servicios (analistas), es que éstos buscan el mejor producto disponible en el mercado. Por el contrario, en el mercado empresarial (donde Cisco mantiene su supremacía) una marca fuerte y un canal de distribución sólido suelen ser los factores decisivos. Además, los proveedores de servicios piensan construir sus redes utilizando equipo de una amplia gama de proveedores. Este no es el *modus operandi* predilecto de muchos administradores de redes corporativas, quienes prefieren utilizar el mismo proveedor en toda su red.

El servicio al cliente es también un factor en la caída de Cisco. Las compañías más pequeñas de redes pueden brindar un servicio más personalizado que Cisco a los proveedores individuales de servicios: es imposible para Cisco administrar decenas de miles de cuentas empresariales. Por otro lado, esto se compensa brindando atención individualizada a media docena de clientes.

Estudio de caso

Una compañía nueva que se está haciendo de un buen nombre es Juniper Networks, de Mountain View, California, que hace su propia línea de enrutadores de alta velocidad. Desde su fundación, en junio de 1999, hasta el 2001, sus acciones crecieron 494%, superando el 118% de incremento de Cisco durante el mismo periodo. Los pesimistas, que pensaron que se trataba de otra empresa de las llamadas dot.com, se vieron forzados a reconsiderarla. Juniper tiene ventas reales. En 1998, Cisco controlaba el 86.6% de un mercado valuado en 175 millones de dólares anuales de enrutadores de alta velocidad. Por esas mismas fechas, Juniper tenía 6% de participación en el mercado. Sólo un año después, Juniper había aumentado 17.5% su participación del total, que era de 578 millones de dólares. De acuerdo con Dataquest, Cisco descendió a 80.7%. Juniper ha experimentado muchos altibajos, similares a los de Cisco, en los primeros años de ésta década. Sin embargo, al igual que Cisco, Juniper ha sabido capotear el temporal.

La supremacía de Juniper sobre Cisco se debe a la confiabilidad de su hardware y a su administración corporativa. Además, a menudo se reconoce que el software de administración de tráfico JUNOS de Juniper es más confiable que el sistema IOS de Cisco. Como es natural, Cisco no está de acuerdo con esta afirmación, pero los números todavía causan preocupación en San José.

Sin embargo, lo que más importa es que el IOS de Cisco es por mucho el sistema operativo para dispositivos de interconectividad que más se ha instalado. Lo anterior ha llevado a que muchas personas que toman decisiones en las empresas vean a Cisco como la opción más segura, porque es más probable que los miembros del mercado laboral de la interconectividad estén más entrenados en el IOS que en cualquier otro entorno.

¿Quién desea ser millonario?

Para muchas compañías en el campo de la tecnología, la panacea del éxito no está sólo en el desarrollo y la venta de un gran producto que la gente utilice todos los días. Otra posibilidad es que la compañía reciba la bendición de Cisco, y que luego la adquiera. A su debido tiempo, esto transforma de manera instantánea a los ejecutivos y empleados de la compañía en millonarios (sin necesidad de ganar algún *reality show*).

Adquisiciones

Cisco no es un extraño en el campo de las adquisiciones, porque construyó su enrutador, su equipo de seguridad para conmutadores, su equipo inalámbrico y sus líneas para VoIP con tecnología que adquirió de otras empresas.

En 1999 y 2000, Cisco compraba compañías en menos tiempo del que le tomaba poner el nombre de la empresa en papel membretado. Luego estalló la burbuja de la tecnología y Cisco puso un freno a sus adquisiciones. De manera lenta pero cautelosa, Cisco ha tomado su paso en cuanto a compras y en el 2005 había adquirido una docena de compañías e invertido alrededor de 805 millones de dólares ese año.

Una de sus adquisiciones más jugosas se dio a principios de enero del 2005, cuando compró Airespace, un proveedor de conmutadores inalámbricos para LAN, por 450 millones de dólares. A pesar de que Cisco ya tenía un portafolio robusto de productos inalámbricos, Airespace reforzó su línea de productos con dispositivos fáciles de usar, configurar y administrar. Quizás aún más importante es el impacto positivo en cuanto a seguridad que Airespace le brindó al catálogo de productos inalámbricos de Cisco.

Los analistas prevén que Cisco adquirirá todavía más tecnología en los meses y años por venir.

Software

Cisco no se limita a comprar hardware. Casi la mitad de las adquisiciones que realizó en el 2004 fueron de software, entre las que se incluyen a Protego y Perfigo, que fabrican software de administración e imposición de seguridad; Dynamicsoft fabrica software de administración para VoIP; Jahai Networks crea aplicaciones para la administración de redes; y Twingo desarrolla aplicaciones de seguridad para computadoras de escritorio.

Los analistas del mercado esperan que Cisco adquiera en el futuro software para ofrecer servicios de video por demanda, software de administración de redes para la virtualización de recursos de centros de datos y nuevas aplicaciones para la administración de la entrega de servicios.

Es probable que Cisco esté vislumbrando mejorar sus productos de aceleración de datos, en especial en el campo del tráfico y seguridad de XML (eXtensible Markup Language). En relación con la aceleración, es probable que Cisco también esté vislumbrando adquirir compañías que se especialicen en la optimización del ancho de banda de las redes WAN.

Mientras que Cisco hace grandes y pequeños negocios con sus adquisiciones, aparentemente tiene la mejor de las suertes con algunas de las más pequeñas (menos de un mil millones de dólares, si esa cantidad le parece pequeña). Por ejemplo, la compra de Aironet en 1999 significó la adquisición de equipo inalámbrico extremadamente popular y rentable.

Scientific-Atlanta

Sin embargo, la adquisición que ha tenido implicaciones de mayor alcance (al menos para el público general) fue la que hizo Cisco de Scientific-Atlanta, la compañía que fabrica decodificadores para cable, en seis mil 900 millones de dólares. Esta adquisición está empatada con la más grande de Cisco (compró la compañía óptica Cerent en 1999, al mismo precio).

Esta compra de alguna manera está fuera de la tendencia de Cisco. Históricamente, las adquisiciones de Cisco han sido pequeñas compañías en Silicon Valley. Como lo indica su nombre, esta compra está en el lado opuesto del país y es una compañía grande.

La adquisición es una jugada estratégica de Cisco, porque las compañías de cable están luchando por una posición en el mercado de video bajo demanda IPTV e IP. Debido a que esos operadores ya utilizan equipo de Cisco en sus cabezales de video, la instalación de equipo Cisco en las casas de los consumidores representa una estrategia inteligente.

Expansión del portafolio

Cisco continúa expandiendo y desarrollando su tecnología y su oferta de productos mediante la adquisición de compañías promisorias con lo último en tecnología y servicios. Algunas veces, las adquisiciones de Cisco pueden impulsar o eliminar una tecnología. Por ejemplo, cuando empezó la especulación para ver si ATM podría o debía tomar el liderazgo en la tecnología de espina dorsal más popular, muchos analistas supusieron que Cisco (una compañía con gran historial en Ethernet) podría combatir con Gigabit Ethernet. En cambio, Cisco adquirió StrataCom, la compañía número uno en tecnología ATM, en una de las fusiones tecnológicas más grandes que se habían visto. Cisco también ha comprado proveedores de software enfocados en suministrar soluciones en las áreas de administración y diseño de redes. Por muchos años, Cisco se ha promovido como el principal comercializador de soluciones para la conectividad empresarial de la industria, y su deseo de adaptarse a las tendencias tecnológicas, en lugar de luchar contra ellas, ha impresionado a los analistas.

En la tabla 1-1 se muestran las adquisiciones de Cisco, del 2001 al 2005, junto con una breve descripción de lo que fabrican y hacen.

Fecha de la adquisición	Nombre	Descripción
29 de nov., 2005	Cybertrust	Servicio de información de inteligencia para la seguridad llamado Intellishield Alert Manager.
18 de nov., 2005	Scientific-Atlanta	Tal vez la adquisición con el mayor potencial para Cisco. Este fabricante de equipo digital de televisión por cable puede ayudar a Cisco a encontrar un lugar en los televisores de todo el público.
30 de sep., 2005	Nemo Systems	Compañía de semiconductores que desarrolla circuitos de memoria para redes.

Tabla 1-1. Adquisiciones de Cisco de 2001 a 2005. (*Continúa*.)

Fecha de la adquisición	Nombre	Descripción
22 de julio, 2005	KISS Technology	Proveedor tecnológico para dispositivos de entretenimiento de red.
27 de junio, 2005	Netsift	Soluciones de procesamiento de paquetes a alta velocidad.
14 de junio, 2005	M.I. Secure Corporation	Soluciones de seguridad y VPN.
26 de mayo, 2005	FineGround Networks	Equipos de red que aceleran, aseguran y supervisan la entrega de aplicaciones.
23 de mayo, 2005	Vihana	Soluciones en semiconductores.
27 de abril, 2005	Sipura Technology	Especialistas en VoIP.
14 de abril, 2005	Topspin Communications	Conmutadores para servidores.
12 de enero, 2005	Airespace	Dispositivos LAN inalámbricos.
20 de dic., 2004	Protego Networks	Software para la seguridad de redes.
9 de dic., 2004	BCN Systems	Software flexible para enrutamiento.
17 de nov., 2004	Jahi Networks	Dispositivos para la administración de redes.
21 de oct., 2004	Perfigo	Control de acceso a redes.
13 de sept., 2004	Dynamicsoft	Software SIP.
9 de sept., 2004	NetSolve	Administración de la infraestructura de IT.
23 de agosto, 2004	P-Cube	Plataformas para el control del servicio IP.
8 de julio, 2004	Parc Technologies	Soluciones de ingeniería de tráfico y software para la optimización del enrutamiento.
29 de junio, 2004	Actona Technologies	Soluciones para redes de almacenamiento.
17 de junio, 2004	Procket Networks	Tecnologías de silicio para enrutadores.
22 de marzo, 2004	Riverhead Networks	Software distribuido para ataque de negación del servicio.
12 de marzo, 2004	Twingo Systems	Seguridad en computadoras de escritorio con SSL y VPN.
12 de nov., 2003	Latitude Communications	Conferencias de audio y Web.
20 de marzo, 2003	Linksys Group	Dispositivos para el consumidor casero y de pequeñas oficinas.

Tabla 1-1. Adquisiciones de Cisco del 2001 a 2005 (*continúa*).

Fecha de la adquisición	Nombre	Descripción
19 de marzo, 2003	SignalWorks	Software para la cancelación de eco.
24 de junio, 2003	Okena	Software para la detección de intrusos.
22 de oct., 2002	Psionic Software, Inc.	Software para la detección de intrusos.
20 de agosto, 2002	Andiamo Systems	Sistemas de conmutación para el almacenamiento.
25 de julio, 2002	AYR Networks	Software para redes distribuidas.
1 de mayo, 2002	Navarro Networks	Diseño de ASIC para Ethernet.
1 de mayo, 2002	Hammerhead Networks	Diseño de software para redes.
27 de julio, 2001	Allegro Systems	Aceleración de VPN.
11 de julio, 2001	AuroraNetics	Compañía de tarjetas de chips RPR.

Tabla 1-1. Adquisiciones de Cisco del 2001 a 2005 (*conclusión*).

Soluciones de Cisco

Cisco se promociona como el principal "proveedor de soluciones empresariales de extremo a extremo" en interconectividad. Lo que esto significa en español es que Cisco tiene una amplia funcionalidad en su línea de productos para satisfacer casi cualquier necesidad de sus clientes, ya sea voz/datos integrados, espinas dorsales de ATM o la integración a ambientes SNA de IBM, etcétera. En términos prácticos, Cisco ha sido capaz de hacer esto debido a su visión a largo plazo y su flujo de efectivo. El poseer más de 180 mil millones de dólares en capitalización del mercado a finales de 2003, le proporcionó la fortaleza financiera para llenar los huecos de su línea de productos e ingresar al campo de las nuevas tecnologías, ya sea por medio de la investigación y el desarrollo intensivos dentro de la compañía, o saliendo a adquirir las mejores empresas proveedoras de tecnología. Como se mencionó, Cisco ha comprado más de 70 compañías en los últimos años. Cada adquisición parece haberse realizado para asimilar una nueva tecnología y no para comprar la base de clientes de las pequeñas compañías.

No todas las tecnologías de soluciones de Cisco han sido resultado de adquisiciones; algunas se desarrollaron internamente. Sin embargo, gran parte de las adiciones de tecnologías principales se hicieron mediante adquisiciones. El factor clave en cada una de ellas ha sido si Cisco puede integrar con éxito la nueva tecnología a la arquitectura IOS unificadora de la compañía (también conocida como *fusión*). A pesar de los deseos de ciertos competidores, hasta el momento Cisco ha hecho un magnífico papel al respecto, salvo algunas excepciones. A continuación se muestra un panorama de las áreas de soluciones más importantes:

- **Conjuntos de características de IOS** El IOS puede comprarse a la carta para muchos dispositivos, con el fin de obtener la funcionalidad necesaria para satisfacer las necesidades del ambiente que tiene instalado el cliente, ya sea desde SNA de IBM, NetWare de Novell, AppleTalk o simple IP.
- **ATM** Cisco ha invertido grandes sumas de dinero en tecnología ATM, con la compra de StrataCom trajo una línea completa de conmutadores ATM WAN, conmutadores ATM multiservicio y concentradores de extremo. Asimismo, Cisco también compró una compañía llamada LightStream para obtener el módulo de ATM LightStream 1010 para conectarse a las LAN de campus ATM.
- **Integración de voz/datos** Para consolidar su posición en el mercado VoIP emergente, Cisco ofrece el conmutador de voz/datos abierto programable VCO/4K, la compuertas conmutadas Cisco-a-circuito y otros productos para integrar la voz.
- **Administración de redes** Algunas aplicaciones de software de administración dispares, tanto fabricadas internamente como adquiridas por fuera, se están mezclando poco a poco bajo el nombre CiscoWorks. Por el momento, las cosas están un poco en desorden y sólo existen tres productos más o menos independientes: Resource Manager Essentials para administrar redes enrutadas, CWSI Campus para administrar redes de conmutadores y NetSys Baseliner para diseñar topologías de redes. CWSI y NetSys fueron adquisiciones. De manera adicional, la administración de la seguridad se maneja por medio de CS-MARS, que fue el resultado de la adquisición de Protego.
- **Conectividad ISP** Cisco ofrece productos "directores" para que los ISP los utilicen para manejar sus altos volúmenes de tráfico. LocalDirector de Cisco es un sistema sofisticado de administración de conexiones de servidor que maneja el tráfico con base en la solicitud de servicio, método de distribución y disponibilidad del servidor. El Distributed-Director de Cisco es similar, pero proporciona una administración dinámica y transparente de la distribución del tráfico de Internet entre servidores dispersos geográficamente.
- **Seguridad** CiscoSecure es el sistema de administración de seguridad cliente-servidor integrado de la compañía. El propio IOS por sí mismo incorpora muchos comandos de seguridad en el nivel del dispositivo cliente y CiscoSecure conserva una base de datos central de usuarios, autorizaciones de usuarios y el historial de eventos respecto a la seguridad. Cisco ofrece el PIX Firewall para la seguridad en el tráfico y el Cisco ASA para tráfico y seguridad de la aplicación. Para quienes acceden a una red a través de Internet, Cisco ofrece soluciones VPN que se equiparan con los productos de Cisco, que están incluyendo cada día más funcionalidad VPN. Cisco también ofrece un conjunto de características de IOS llamado Firewall IOS y Secure ACS, que en esencia es un conjunto extendido de comandos de IOS que permiten la configuración de casi todos los enrutadores de rango medio y elevado de Cisco con funcionalidad de firewall.
- **Redes de almacenamiento de área (SAN)** El grado de funcionalidad de una red de computadoras no se relaciona únicamente al hecho de que todos tengan una computadora en una organización o que la red es más rápida que un relámpago. El material que recorre la red (es decir, los datos) debe estar almacenado en algún lugar. En organizaciones que tienen la necesidad de almacenar y conservar una gran cantidad de información, las redes de almacenamiento de área (SAN) son

una opción cada vez más popular. Las SAN son plataformas de comunicaciones que interconectan servidores y dispositivos de almacenamiento a velocidades de gigabits. Productos como la serie MDS 9000 de Cisco de conmutadores multicapa ayudan a proporcionar un entorno en que se puede conservar la información.

- **Redes de contenido** Con la finalidad de proporcionar acceso a contenido específico de la red, muchas organizaciones están implantando soluciones de red de contenido, que ofrecen una manera inteligente de enrutar contenido donde sea necesario. Por ejemplo, las redes de contenido ayudan a promover el aprendizaje electrónico, los medios de comunicación y la distribución de archivos. Cisco ha desarrollado un gran número de herramientas y tecnologías para facilitar la conectividad de contenido, entre las que se incluye la Content Engine 7300, que acelera la entrega de contenido, mejorando su escalabilidad y disponibilidad.
- **Inalámbrico** Hace unos años, la tecnología de red inalámbrica hubiera parecido demasiado costosa como para representar una opción factible de trabajo en red. Sin embargo, en la actualidad, la tecnología inalámbrica está al alcance de todos y muchas computadoras incluyen tarjetas inalámbricas ya instaladas. Cisco no es un extraño en el mundo de la tecnología inalámbrica, al desarrollar su propia línea de productos empresariales. Sin embargo, la compañía también ha extendido su alcance al campo de la conectividad inalámbrica de los hogares y los pequeños negocios mediante la adquisición de Linksys en el 2003.
- **Voz sobre IP (VoIP)** Las redes de computadoras no sólo son útiles para el transporte de información entre servidores y clientes. Mediante la utilización del famoso protocolo Internet (IP), se pueden realizar llamadas telefónicas entre redes de computadoras utilizando telefonía IP. Cisco ofrece gran cantidad de dispositivos que facilitan la VoIP, desde auriculares conectados a conmutadores hasta teléfonos IP inalámbricos o conmutadores y enrutadores con capacidad de VoIP. VoIP es una tecnología popular porque permite tener un servicio de telefonía a costo muy bajo dentro de la organización (ya sea que la empresa se encuentre dentro de un edificio o distribuida en sucursales alrededor del mundo).
- **Distribución de video** La entrega de video a través de las redes abarca multimedia y videoconferencia. Cualquier persona que haya visto una película en su computadora o que haya descargado un archivo MP3, sabe el tamaño de esos archivos. Cisco facilita su entrega y administración con sus sistemas Video Portal y Video Portal Manager.

A lo largo de este libro se estudiarán éstas y otras soluciones de Cisco. No las abordaremos aquí con gran detalle; necesita conocer datos técnicos primero. Este proceso comienza en el próximo capítulo (una introducción a los fundamentos de la tecnología de la interconectividad).

CAPÍTULO 2

Introducción a las redes

¿Alguna vez se ha preguntado cómo funciona realmente Internet? En un momento u otro, la mayoría de nosotros nos hemos preguntado qué está sucediendo tras el telón cuando navegamos entre páginas Web, enviamos correo electrónico o descargamos archivos. De manera instintiva, sabe que debe haber muchos dispositivos que lo conectan a otra computadora, pero ¿cómo se realiza en realidad la conexión? ¿Cómo está integrado un mensaje y cómo encuentra un camino de regreso a nuestra computadora entre esa red aparentemente caótica que es Internet? Después de todo, no ha pasado mucho tiempo desde que la incompatibilidad entre las diferentes marcas y modelos de computadoras hicieron que el intercambio de datos fuera un dolor de cabeza. Ahora todos pueden conectarse a Internet para compartir datos y servicios sin pensarlo mucho. ¿Cómo hizo esto posible la industria de la computación?

La mayoría de las personas que no saben mucho de computadoras cree que la respuesta es la tecnología, y hasta cierto punto tiene razón. Sin embargo, la respuesta completa es que Internet se formó por medio de la combinación de tecnología y estándares (específicamente, estándares técnicos *de jure* y *de facto*). Los estándares *de jure* los establecen las asociaciones comerciales; los *de facto* los establece la fuerza económica bruta. Ni todos los enrutadores y conmutadores del mundo hubieran podido desarrollar Internet sin estándares que hicieran posible la compatibilidad entre el software, el hardware y el equipo de telecomunicaciones.

Los productos que hicieron posible Internet se presentaron en el capítulo 1. Ahora estudiaremos las arquitecturas que hicieron posible toda esa tecnología. Una comprensión de las tecnologías y los estándares que sustentan una interconexión le brindará un panorama muy claro de lo que sucede tras bambalinas cuando hace clic en un vínculo de su navegador.

BITS Y BYTES

Antes de abordar los detalles de la interconectividad, es necesario cubrir los conceptos básicos que explican cómo funciona la tecnología de las computadoras. Haremos esto partiendo de lo más elemental, con el fin de que comprenda por qué los sistemas trabajan como lo hacen.

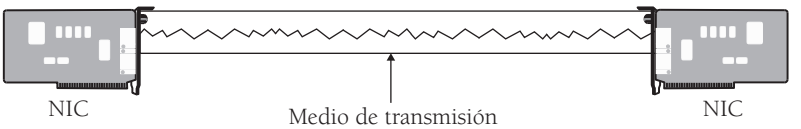
La infraestructura de Internet está compuesta por millones de dispositivos de red (enrutadores, conmutadores, firewalls, servidores de acceso y concentradores) conectados entre sí por medio de un sofisticado sistema de direcciones globales. Se encuentran conectados principalmente con cables de cobre de par trenzado a las computadoras de escritorio y mediante líneas troncales de gran tamaño que corren por cables de fibra óptica de muy alta velocidad. Pero, en esencia, Internet es cuestión de millones de dispositivos de hardware individuales conectados entre sí por medio de un esquema de direccionamiento global.

Cómo interpretan los datos las computadoras

Los dispositivos para red son más o menos los mismos con los que cuentan las plataformas de cómputo normales, como su PC. Las mayores diferencias radican en la configuración: casi todos los tipos de equipo de red no cuentan con monitores ni discos, porque están diseñados para transferir datos (no para almacenarlos y presentarlos). Sin embargo, todos los dispositivos de red son computadoras, en el sentido de que tienen CPU, memoria y sistemas operativos.

Los bits forman mensajes binarios

De lo que se trata la computación, en gran medida, es de enviar señales eléctricas entre varios componentes de hardware. En una plataforma de cómputo estándar, las señales salen disparadas de los pequeños transistores que están dentro de la CPU o memoria y viajan por alambres muy pequeños instalados en tarjetas de circuito impresas. Una vez afuera, las señales eléctricas viajan por los cables para desplazarse entre los dispositivos.



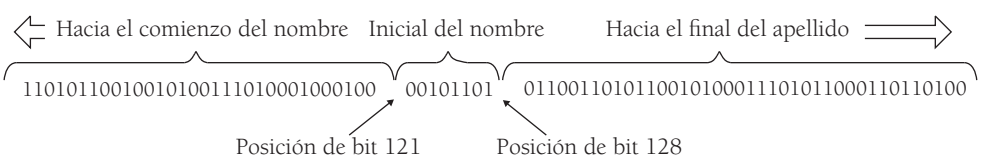
A medida que las señales se transfieren por el cable, las tarjetas de interfaz de red (NIC), que se encuentran en cada extremo, registran las formas de onda de los pulsos eléctricos y las interpretan como datos. La NIC interpreta cada pulso eléctrico como una señal de encendido o apagado. A esto se le denomina transmisión *binaria* (un sistema en que cada pulso Encendido se registra como un 1 y cada pulso Apagado como un 0). En lenguaje de máquina, estos ceros y unos son *bits* y un archivo de bits es un archivo *binario*.

Las fluctuaciones de voltaje de los pulsos eléctricos (o los pulsos de luz, en el medio de transmisión de fibra óptica), durante intervalos minúsculos, determinan si una señal representa un cero o un uno. A estos pequeños intervalos se les conoce como *ciclos por segundo*, o Hertz (Hz) en los círculos de la ingeniería eléctrica. Por ejemplo, la CPU de una NIC a 100 Mbps puede generar 100 millones de ciclos por segundo. En términos prácticos, la computadora puede procesar 100 millones de pulsos por segundo e interpretarlos como ceros o unos.

Cómo se conserva el orden entre los bits

Todas las computadoras utilizan transmisión binaria. Los bits son la materia prima básica con la que trabajan, por lo general como una colección de bits en un archivo binario. Los archivos binarios son los que se colocan en la memoria, se procesan en las CPU, se almacenan en discos y se envían por los cables. Tanto los datos como los programas de software se almacenan como archivos binarios. Si pudiera ver los archivos de datos en formato binario en cualquier tipo de computadora, vería una página llena de ceros y unos. Esto provocaría que sus ojos se nublaran, pero las computadoras pueden trabajar con este formato binario debido a la *ordinalidad* (un término gracioso asignado para saber qué parte de la información debe aparecer en una cierta posición de un campo).

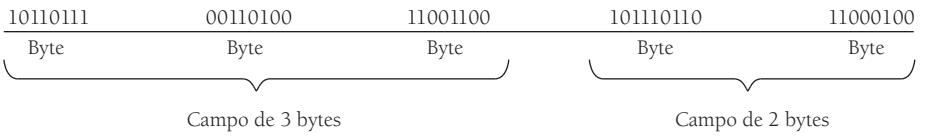
La computadora no conserva un registro de las posiciones ordinales una por una. En cambio, mantiene un registro de la posición de bit en que comienza y termina un campo. Un *campo* es un espacio lógico de información. Por ejemplo, la computadora puede saber que de la posición de bit 121 a la 128 se utiliza para almacenar la inicial del nombre de una persona.



Las computadoras mantienen registro del orden de los bits con gran precisión, utilizando relojes que registran el tiempo exacto donde una CPU se encuentra en un flujo de bits. Al saber dónde se encuentran los campos, las computadoras pueden reconstruir los datos desde el principio.

El software de la computadora opera en bytes

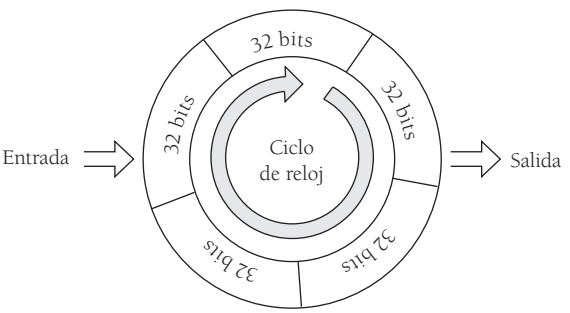
Sin embargo, por simplicidad, las computadoras no procesan bit por bit. Existe un nivel intermedio que se encuentra un escalón arriba del bit llamado byte, de ahí la expresión "bits y bytes". Un *byte* es una serie de ocho bits consecutivos que funcionan como una unidad.



Desde un punto de vista lógico, la unidad básica que conforma un campo de datos es el byte. Esto no sólo hace que los sistemas trabajen más rápido, sino que también los hace más fáciles de programar y depurar. Nunca verá a un programador declarar cuántos bits debe tener un determinado campo, pero declarar la longitud en bytes es una práctica rutinaria. A menudo se le deja a la computadora la tarea de conservar un registro de las posiciones individuales de bit.

Palabras de computadora

A diferencia del software, la CPU debe trabajar en bits. En el nivel más bajo, el hardware de la computadora trabaja con señales eléctricas de encendido/apagado en forma de bits que viajan por su circuitería. Tomaría mucho tiempo realizar la conversión de bits a bytes dentro de la CPU, por lo que las computadoras cuentan con algo denominado *tamaño de palabra*. El escalón que se encuentra arriba de un byte es la *palabra*, que representa el número de bytes que una determinada arquitectura de CPU está diseñada para manejar en cada ciclo.



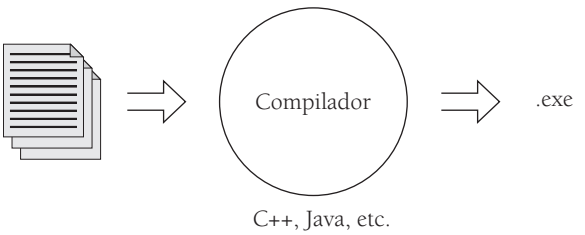
Palabra de 32 bits en la CPU

Por ejemplo, una PC o un servidor basado en el procesador Xeon de Intel, es una máquina con una longitud de palabra de 32 bits, lo que significa que procesa 32 bits por cada ciclo de reloj. Sin embargo, a medida que las técnicas de minituarización del hardware han avanzado (y la necesidad de procesar datos más rápidamente ha aumentado), la industria ha adoptado arquitecturas de 64 bits como estándar. Existe una gran variedad de máquinas

de 64 bits disponibles de diferentes proveedores, como IBM, Sun y fabricantes que utilizan la arquitectura Itanium 2 de Intel. Los dispositivos Cisco utilizan CPU de 32 y 64 bits.

Software compilado

El último escalón debe llevar de los bytes a algo que el ser humano pueda comprender. Como tal vez ya lo sepa, el software toma la forma de archivos de código fuente escritos por los programadores de computadoras. Los comandos que los programadores teclean para formar archivos de código fuente son símbolos que dan instrucciones a la computadora de lo que deben hacer. Cuando se escribe un programa, éste se convierte en lenguaje de máquina (bits y bytes) por medio de un programa *compilador*, que es una aplicación especializada que traduce el código de software en archivos de lenguaje máquina conocidos como *ejecutables* o *binarios*. Por ejemplo, si se escribe código con el lenguaje de programación C++, éste se traduce por medio de un programa compilador de C++.



Ya se habrá dado cuenta de que en el directorio de su PC existen archivos con extensiones .exe y .bin. Son abreviaturas de *ejecutable* y *binario*, respectivamente. El IOS (sistema operativo de interconectividad) de Cisco es software ejecutable. En realidad, se trata de un paquete que contiene cientos de ejecutables que sirven para poner en operación el hardware de los dispositivos, reenviar paquetes, hablar con dispositivos de redes vecinas, etcétera.

Arquitecturas de cómputo

Una *arquitectura de cómputo* es una especificación técnica de todos los componentes que integran un sistema. Las arquitecturas de cómputo publicadas son muy detalladas y específicas, y casi todas abarcan miles de páginas. Pero en ciertas partes, son abstractas por diseño, dejando al diseñador la implantación exacta de esta porción de la arquitectura.

Función
Funcionalidad
Distribución
Apariencia
Interfaz abstracta
Dependencias
Extensiones
Productos
Implementación

Lo que separa a una arquitectura de una especificación normal de un producto es el uso de la capa abstracta. Una *capa de abstracción* es una interfaz fija que conecta dos componentes del sistema y rige la relación entre la función y la implementación en cada lado. Si algo cambia en un lado de la interfaz, por diseño no deberá cambiar en el otro lado. Estas capas se colocan para ayudar a garantizar la compatibilidad en las dos direcciones:

- ▼ Entre varios componentes en el interior del sistema.
- ▲ Entre varios productos que implementan la arquitectura.

Una abstracción entre componentes estabiliza los diseños del sistema, porque permite que diferentes grupos de desarrollo trabajen en la ingeniería sobre un objetivo estable. Por ejemplo, la interfaz publicada entre las capas en el software de red permite que cientos de fabricantes de interfaces de red diseñen productos compatibles con la especificación Fast Ethernet.

Existen varias arquitecturas de cómputo importantes (algunas más abiertas que otras). La arquitectura de Microsoft Windows/Intel 80x86 Wintel es una arquitectura legendaria. Otras importantes son RAID (arreglo redundante de discos económicos), Java, CORBA (arquitectura de corredor de solicitud de objeto común, una arquitectura e infraestructura de fabricante independiente que utilizan las aplicaciones para trabajar juntos en red) y una docena más. Quizás la arquitectura de cómputo más importante que jamás se haya ideado es la que creó Internet: el modelo de referencia OSI.

MODELO DE REFERENCIA OSI

La International Organization for Standardization (ISO), una organización internacional de ingeniería con oficinas principales en París, publicó por primera vez en 1978 el modelo de referencia para la interconexión de sistemas abiertos (OSI). Este modelo de siete capas se ha convertido en el estándar para el diseño de métodos de comunicación entre dispositivos de red y fue la guía que se utilizó para diseñar el protocolo Internet (IP).

El objetivo del modelo de referencia OSI fue promover la *interoperabilidad*: la posibilidad de que sistemas incompatibles puedan trabajar juntos, de manera tal que realicen con éxito tareas comunes. Un buen ejemplo de interoperabilidad sería una LAN tipo Ethernet intercambiando mensajes de forma transparente con una LAN tipo Token Ring de IBM.

La pila de siete capas

El modelo OSI divide las redes en siete capas funcionales y, por lo tanto, se le conoce a menudo con el nombre de *pila de siete capas*. Cada capa define una función o grupo de funciones que se llevan a cabo cuando se transfieren los datos entre aplicaciones en red. No importa que el protocolo de red sea IP, NetWare de Novell o AppleTalk, si se adhiere al modelo OSI, se aplicarán más o menos las mismas reglas en cada una de las siete capas. Las siete capas se muestran en la figura 2-1.

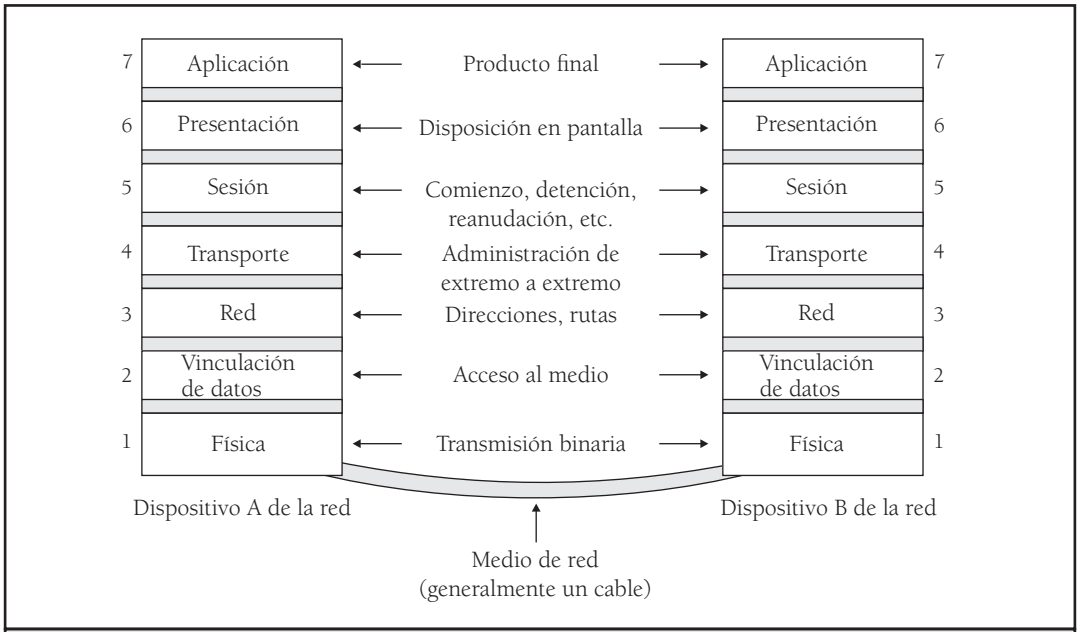


Figura 2-1. Cada capa del modelo OSI activa protocolos para administrar conexiones entre dispositivos.

Las capas

Como se muestra en la figura 2-1, cada capa es un protocolo de comunicaciones entre los dispositivos que están conectados. En relación con las operaciones de red, lo que es importante comprender es que cada capa de cada dispositivo se comunica con su homólogo para administrar un aspecto particular de la conexión de red. En relación con la interoperabilidad, la clave es la interfaz fija que reside entre cada capa. Las capas abstractas reducen lo que de otra forma sería demasiado complejo.

- **Capa 1, la capa física** Controla el medio de transporte, al definir las características eléctricas y mecánicas que transportan la señal de datos. Algunos ejemplos son los cables de par trenzado, de fibra óptica y coaxial, y las líneas en serie.
- **Capa 2, la capa de vinculación de datos** Controla el acceso a la red y asegura una transferencia confiable de marcos en red. La especificación de circulación de datos más conocida es el acceso múltiple de percepción de portadora con detección de colisiones (CSMA/CD) de Ethernet. Tanto Token Ring como la interfaz de datos distribuidos por fibra (FDDI) se adhieren a la arquitectura de vinculación de datos de paso de ficha.
- **Capa 3, la capa de red** Administra el desplazamiento de datos entre diferentes redes. Los protocolos de esta capa son responsables de encontrar el dispositivo al que están destinados los datos. Como ejemplos se incluye el protocolo IP, el intercambio de paquetes de interconexión (IPX) y AppleTalk.

- **Capa 4, la capa de transporte** Asegura que los datos lleguen a su destino intactos y en el orden correcto. El protocolo de control para la transmisión (TCP) y el protocolo de datagrama de usuario (UDP) trabajan en esta capa.
- **Capa 5, la capa de sesión** Establece y termina conexiones y organiza sesiones entre dos computadoras. Algunos ejemplos de protocolos de la capa de sesión son la llamada a procedimiento remoto (RPC) y el protocolo ligero de acceso a directorios (LDAP).
- **Capa 6, la capa de presentación** Forma los datos para desplegarlos en la pantalla o imprimirlos. Ejemplos de protocolos de la capa de presentación son el protocolo ligero de presentaciones (LPP) y NetBIOS.
- ▲ **Capa 7, la capa de la aplicación** Contiene los protocolos que se utilizan para llevar a cabo tareas importantes en una red. Algunos ejemplos de protocolos en esta capa son el protocolo de transferencia de correo simple (SMTP) para correo electrónico, el protocolo de transferencia de hipertexto (HTTP) para navegadores Web y servidores, Telnet para sesiones entre terminales remotas, y cientos más.

Las aplicaciones de red de la capa 7 son la razón por la que existen las seis capas inferiores. Muchos de estos protocolos se utilizaron por primera vez en sistemas UNIX, dado que este sistema operativo se desarrolló en paralelo con Internet.

NOTA No se confunda con el nombre "capa de la aplicación". Esta capa ejecuta aplicaciones de red, no de software, como hojas de cálculo o inventarios. Entre las aplicaciones de red se incluyen el correo electrónico, el navegador Web (HTTP), FTP y otras funciones de red importantes.

Capas iguales forman vínculos virtuales independientes al protocolo

Cada capa de la pila depende de las capas superiores e inferiores, pero cada una trabaja de manera independiente, como si mantuvieran una comunicación exclusiva con su capa homóloga de la otra computadora. Se dice que cada capa del dispositivo establece un *vínculo virtual* con la misma capa en el otro dispositivo. Cuando los siete vínculos virtuales se encuentran funcionando, se establece una *conexión de red* y los dos dispositivos se comunican como si estuvieran conectados directamente.

Por ejemplo, en la figura 2-2, la computadora emisora, la PC Wintel del lado izquierdo (Host A) procesa hacia abajo en la pila para enviar un mensaje y el mainframe IBM (Host B) recibe el mensaje procesándolo hacia arriba para interpretar los datos (una solicitud FTP de descarga, en este ejemplo). Luego, las computadoras invierten el proceso, recorriendo sus pilas en sentido contrario, esta vez, para que el mainframe de IBM descargue el archivo en la PC Wintel mediante la aplicación FTP.

En la figura 2-2, se empieza a observar cómo Internet pudo interconectarse con las computadoras del mundo. Debido a que las capas se abstraen y son independientes una de la otra, la aplicación FTP puede ejecutarse en diferentes implantaciones del modelo OSI, en este ejemplo, Ethernet y Token Ring. Observará que a la aplicación FTP no le importan las incompatibilidades inherentes entre los mainframes Windows XP e IBM, ni las que existen entre las tecnologías de red Ethernet y Token Ring. Su única preocupación es que los dispositivos conectados puedan usar FTP para comunicarse de acuerdo con las reglas del modelo OSI.

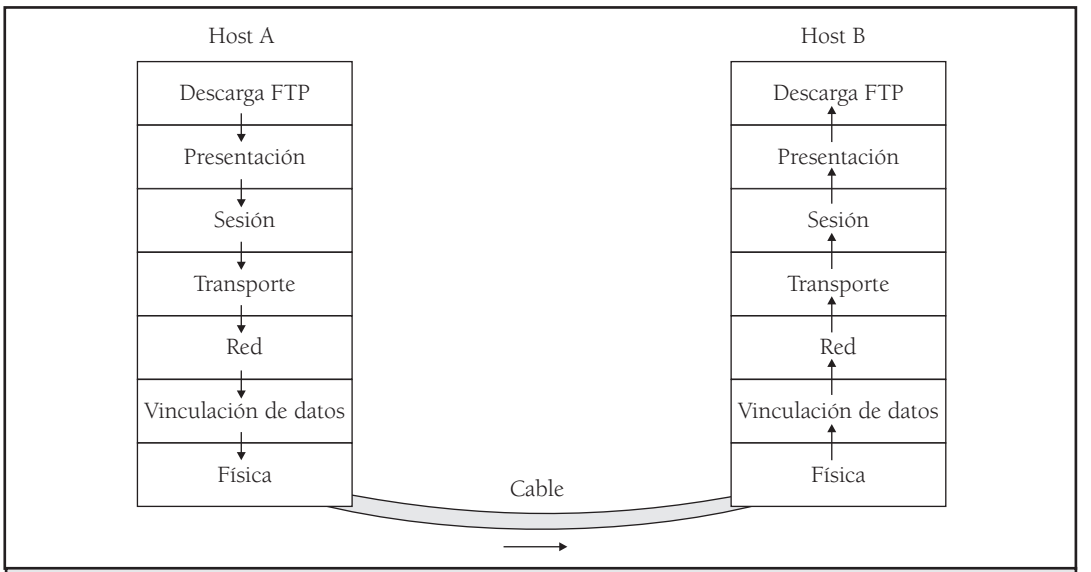


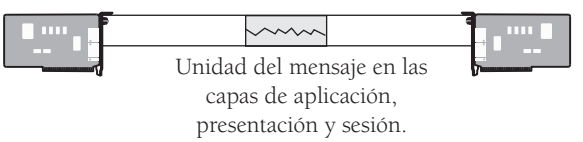
Figura 2-2. Los mensajes se procesan hacia arriba y hacia abajo a través de la arquitectura de las siete capas.

Implementación OSI por capa

Aunque la pila de siete capas se expresa en términos verticales, su observación horizontal ayuda a comprender cómo funciona. Esto es porque, a medida que se procesa un mensaje a través de la pila, su longitud horizontal cambia.

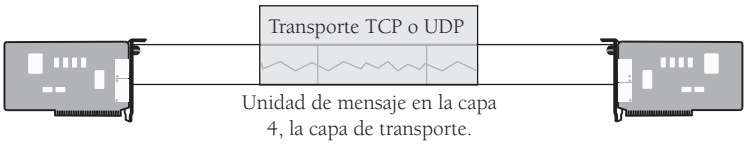
Las primeras tres capas manejan la aplicación horizontal que se está ejecutando (capa de aplicación), los formatos para la representación de los datos (capa de presentación) y la logística de la conexión (capa de sesión). Estas tres primeras capas sólo representan una pequeña porción del mensaje. Por ejemplo, la aplicación que se ejecuta está definida por un número de puerto (la aplicación de página Web HTTP HTML está identificada por el número de puerto 80).

NOTA El nombre "número de puerto" fue una elección poco afortunada por parte de los ingenieros del IETF (Internet Engineering Task Force). Toma un tiempo considerable acostumbrarse al hecho de que un número de puerto IP alude a un tipo de software y no a un puerto de hardware. Una nota relacionada sería que el término "socket" es una dirección IP pareada con un número de puerto.

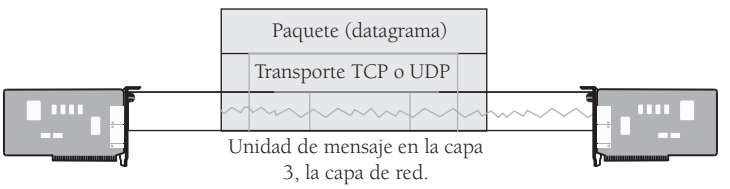


En la capa de transporte, el mensaje se ensancha. Entre las tareas que se realizan en esta capa se incluyen el aseguramiento de que el receptor sabe que el mensaje está por llegar,

que éste no se sature con el envío de muchos paquetes al mismo tiempo, que realmente se reciban los paquetes enviados y que se retransmitan los paquetes que faltaron. Entre los protocolos de transporte se incluyen TCP y UDP en la suite TCP/IP, y la capa de intercambio secuencial de paquetes (SPX) de la suite IPX/SPX de Netware.

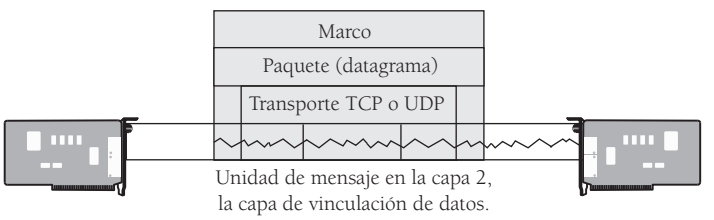


En la capa de red, el mensaje se hace un poco más ancho y se convierte en un *paquete* (también llamado *datagrama*). Cada encabezado de paquete tiene una dirección de red lógica (no física) que se utiliza para enrutar el mensaje por la interconexión. Entre los protocolos de la capa de red se incluyen la parte IP de la suite de protocolos TCP/IP y la capa IPX de la suite de protocolos IPX/SPX de NetWare de Novell, entre otros.



En la capa de vinculación de datos, se lee la información binaria y se encapsula en un formato llamado *marco*. El formato preciso de un marco lo especifica el protocolo de red en que está trabajando la NIC (por ejemplo, Ethernet o Token Ring). Cada encabezado de marco incluye las llamadas direcciones de control de acceso al medio (MAC), que son identificadores únicos que actúan como un tipo de número de serie para dispositivos de hardware.

En el nivel físico, el mensaje es una serie de pulsos. El dispositivo trabaja para codificar o decodificar los pulsos en ceros y unos binarios para comenzar a formar las unidades discretas del mensaje. Este procesamiento de la señal se realiza en el hardware de la tarjeta de interfaz de red, no en el software.



Una vez que se ha eliminado toda la información de protocolos para el manejo del mensaje, lo único que queda son los datos del mensaje. Existe una gran cantidad de unidades individuales del mensaje dentro de una transmisión. Una conexión de red se establece mediante una serie de paquetes, y la información de cada paquete individual contribuye a completar el archivo de datos que necesita la conexión (por ejemplo, una descarga de la página Web).

La carga útil de los datos es variable en cada aplicación. Por ejemplo, una sesión de Telnet enviará archivos pequeños de datos para indicar un teclazo o un retorno de carro, que

pueden incluirse en un paquete o dos. En el otro extremo, una transferencia de archivos FTP puede enviar millones de bytes de datos distribuidos en miles de paquetes.

TECNOLOGÍAS DE RED

Las tecnologías de red (llamadas también tecnologías LAN o especificaciones de red) se utilizan para ejecutar la unidad básica de toda interconexión (el segmento LAN). La tecnología de red más ampliamente conocida es Ethernet, pero existen algunas otras como Token Ring, modo de transferencia Asincrónica (ATM), inalámbrica (WiFi) y FDDI.

Las tecnologías de red están implantadas en la capa de vinculación de datos (capa 2) del modelo de referencia OSI de siete capas. Dicho de otra manera, las tecnologías de red están caracterizadas en gran medida por el medio físico que comparten y la forma como controlan el acceso al medio compartido. Esto cobra sentido si lo piensa detenidamente. La red es conectividad; pero para que se conecte, de alguna forma se debe mantener el orden entre los usuarios que están compartiendo el medio de transmisión. Por esa razón, a la capa 2 (de vinculación de datos) se le conoce como la capa de *control de acceso al medio*, o capa MAC para abreviar. El formato de la unidad del mensaje en este nivel es el *marco de datos* o, simplemente, marco.

Como tales, casi todas las tecnologías de red como Ethernet, Token Ring y FDDI por sí mismas sólo pueden tratar con direcciones MAC (los identificadores de dispositivos que parecen números de serie que ya se mencionaron). Es necesario un protocolo de la capa de red como IP para enrutar mensajes a través de la interconexión. Las tecnologías de red por sí mismas sólo pueden soportar la operación de interconexión conmutada (que sólo es eficiente en áreas locales o rutas simples a grandes distancias, donde no se necesita mucha guía). Las tecnologías de red se utilizan en los extremos opuestos del espectro:

- ▼ **LAN de acceso (distribución)** Aceptan el cableado de dispositivos, conectan grupos de trabajo y comparten recursos como impresoras y servidores departamentales.
- ▲ **LAN de espina dorsal (núcleo)** Vinculan a las LAN de acceso y comparten recursos como servidores de bases de datos, de correo, etcétera.

Las LAN de acceso, formadas por concentradores o conmutadores de acceso, proporcionan a los usuarios y dispositivos interconectividad en un nivel local, por lo general en un piso de un edificio de oficinas. Las LAN de espina dorsal, que están formadas por enrutadores o conmutadores LAN, conectan a las LAN de acceso, normalmente dentro de un edificio o un campus de oficinas. Las interconexiones enrutadas suelen usarse para distribuir tráfico entre las dos.

Ethernet

La versión 1 de Ethernet fue desarrollada por Xerox Corporation a principios de la década de 1970. En la década siguiente, Xerox se asoció con Intel y Digital Equipment Corporation para lanzar la Versión 2, en 1982. Desde entonces, Ethernet se ha convertido en el estándar dominante en tecnología de redes. Primordialmente gracias a las economías de escala, el costo promedio de un puerto Ethernet es ahora mucho menor que el de uno Token Ring. De hecho, Ethernet se ha convertido en un estándar *de facto*, de tal manera que muchos fabri-

cantes están integrando NIC de Ethernet en las tarjetas madre de sus computadoras, para evitar la necesidad de instalar módulos NIC independientes.

Arquitectura de Ethernet

Ethernet opera mediante contención. Los dispositivos que comparten un segmento LAN de Ethernet se mantienen escuchando el tráfico que se transmite por el cable y difiere la transmisión de sus mensajes hasta que el medio esté desocupado. Si dos estaciones hacen sus envíos al mismo tiempo y sus paquetes colisionan, ambas transmisiones se cancelan, las estaciones dejan de enviar y esperan un periodo aleatorio antes de volver a transmitir. Ethernet utiliza el algoritmo CSMA/CD para escuchar el tráfico, detectar colisiones y abortar transmisiones. CSMA/CD es el agente de tránsito que controla lo que de otra forma sería tráfico aleatorio. Restringe el acceso al canal de comunicaciones para asegurar la integridad de las transmisiones. En la figura 2-3 se muestra el proceso CSMA/CD.

Debido a que el medio de transmisión es compartido, cada dispositivo de un segmento LAN de Ethernet recibe el mensaje y lo verifica para ver si la dirección de destino coincide

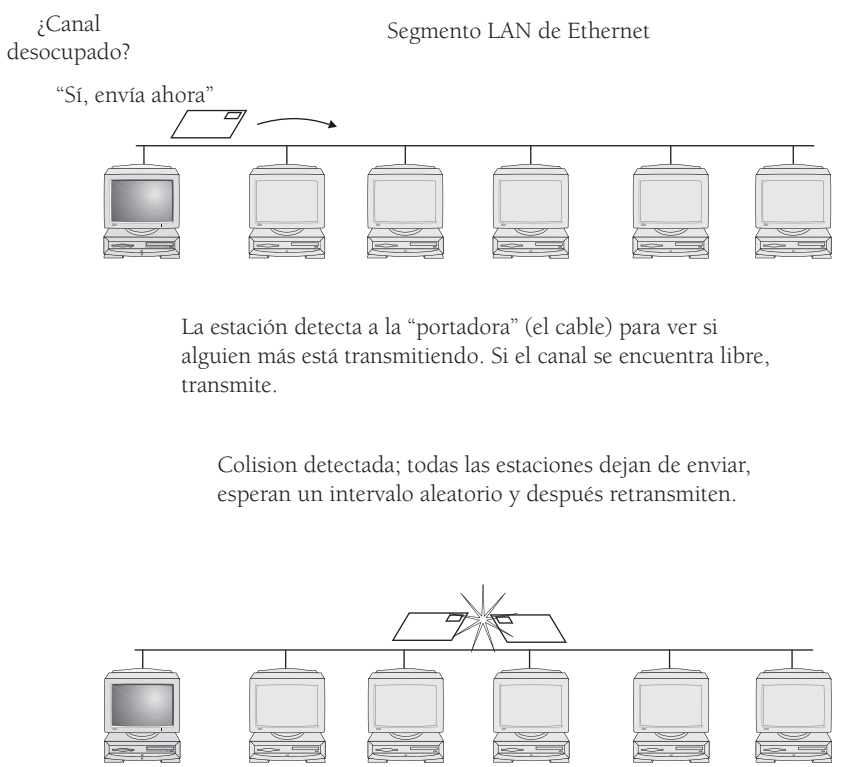


Figura 2-3. El acceso a Ethernet es controlado por la escucha de la portadora y la detección de colisiones del marco.

con su propia dirección. Si es así, se acepta el mensaje, se procesa a través de la pila de siete capas y se establece una conexión de red. Si la dirección no coincide, se elimina el paquete.

NOTA Un algoritmo es una secuencia estructurada de reglas diseñada para manejar procesos variables de una manera ordenada y automática. Los algoritmos son muy comunes en los ambientes de cómputo y redes, porque todo se mueve tan rápido que no queda tiempo para la intervención del ser humano.

Implementaciones de Ethernet

Aun sin economía de escala, Ethernet es más económico, gracias a la naturaleza aleatoria de su arquitectura. En otras palabras, es más sencillo fabricar la electrónica necesaria para operar Ethernet, porque no se intenta controlar todo. En un sentido general, sólo le preocupan las colisiones.

Ethernet cuenta con varias opciones de implementación. La especificación original de Ethernet trabaja a 3 Mbps con cable coaxial o de par trenzado 10BaseT (la letra *T* quiere decir par trenzado; se estudiarán las especificaciones de cableado en el capítulo 6). Fast Ethernet trabaja a 100 Mbps y opera con 100BaseTX o cable de fibra óptica 100BaseFX (la letra *F* corresponde a fibra óptica). Gigabit Ethernet trabaja a 1 000 Mbps (o 1 Gbps) por medio de cable 1000BaseTX o 1000BaseFX. Una opción muy popular de configuración en este momento es utilizar LAN de acceso Fast Ethernet en una LAN de espina dorsal con Gigabit Ethernet.

Gigabit Ethernet y 10 Gigabit

Gigabit Ethernet es una extensión a 1 000 Mbps del estándar de Ethernet. A Gigabit Ethernet se le conoce a veces con el nombre de 1000BaseX, como referencia a la especificación del cableado de fibra óptica y cobre. Gigabit Ethernet está recibiendo promoción de Gigabit Ethernet Alliance, un grupo industrial sin fines de lucro, muy parecido al ATM Forum. El empuje a Gigabit Ethernet está motivado principalmente por su compatibilidad con otras especificaciones de Ethernet (Ethernet a 10 Mbps y Fast Ethernet a 100 Mbps).

Gigabit Ethernet es la principal competencia de ATM para reemplazar a FDDI como la mejor opción de espina dorsal. Su principal ventaja es su familiaridad, dado que Ethernet es la tecnología más extendida. Originalmente diseñada como una tecnología LAN a 1 000 Mbps, Gigabit Ethernet puede escalar a configuraciones WAN. Ethernet utiliza marcos de longitud variable (que van de 64 bytes a 1 518 bytes por marco) y no goza de las características inherentes de QoS "incorporadas" en el protocolo ATM. Sin embargo, muchos administradores de redes votan a favor de Gigabit Ethernet por su facilidad de configuración y uso. Además, no presenta la capa de complejidad agregada que requiere la adaptación LANE (emulación LAN). Forman igual que ATM, las espinas dorsales de Gigabit Ethernet trabajan con gran variedad de tipos de cableado de fibra óptica.

Aunque la conexión Gigabit Ethernet es muy rápida, existe una conexión más rápida en algunos equipos de Cisco, llamada 10 Gigabit Ethernet. Como su nombre lo sugiere, 10 Gigabit Ethernet opera diez veces más rápido que Gigabit Ethernet, a 10 000 Mbps. Mientras que Gigabit Ethernet fue una extensión natural de Fast Ethernet, 10 Gigabit Ethernet difiere en un aspecto importante: el medio físico que se requiere para transportar sus paquetes; 10 Gigabit Ethernet no funciona con cable de par trenzado. Debido a la gran velocidad a la que opera 10 Gigabit Ethernet, por lo general se necesita fibra óptica multimodo o monomodo.

NOTA Hasta el momento de escribir este libro, se encuentra en desarrollo 10 Gigabit Ethernet sobre cobre, y Cisco ya cuenta con modelos disponibles.

En la actualidad, 10 Gigabit Ethernet se utilizará en ambientes de espina dorsal WAN, MAN y de centro de datos (en cualquier lugar donde sea necesario transportar grandes cantidades de datos). Al igual que con cualquier cosa que es nueva y ultrarrápida, los dispositivos 10 Gigabit Ethernet no son económicos. En el extremo superior, el precio de lista de una módulo Catalyst 10GBase-EX4 Metro 10 Gigabit Ethernet es de 79 995 dólares.

El beneficio de estas implementaciones modulares de Ethernet es que los administradores de red puedan impulsar sus inversiones en redes Ethernet. En muchos casos, una organización puede migrar de 10/100 Mbps a Gigabit y 10 Gigabit Ethernet sin tener que reinvertir mucho dinero en su infraestructura.

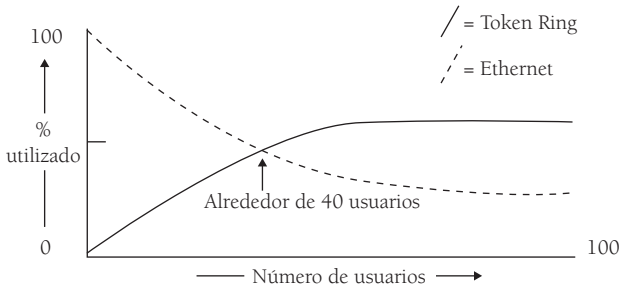
Token Ring

La tecnología Token Ring, casi totalmente desplazada por Ethernet, fue en un tiempo su competencia más importante como estándar para LAN (redes). Fue (y es) un protocolo importante que contó con características dignas de mencionarse. La arquitectura de Token Ring es muy diferente de la de Ethernet.

Como su propio estándar de LAN, Token Ring no es compatible con Ethernet, en cuanto al tipo de NIC y software que debe utilizarse. A pesar de que Token Ring se instaló ampliamente en compañías dominadas por IBM, nunca tuvo éxito como estándar abierto.

Token Ring, que significa anillo de fichas, toma su nombre del hecho que define a los hosts conectados en un anillo lógico. Utilizamos la palabra *lógico* para describir aquí Token Ring, porque el segmento LAN se comporta como un anillo que transfiere señales a la manera de un torneo todos contra todos, como si los dispositivos estuvieran realmente conectados a un cable en forma de anillo. Sin embargo, desde el punto de vista físico, las LAN Token Ring pueden configurarse de una manera llamada *topología de estrella*. En la figura 2-4 se muestra ésta. Tome nota de que, en la terminología de Token Ring, al concentrador de acceso se le denomina *unidad de acceso al medio (MAU)*, en lugar de concentrador.

Token Ring evita la contención en un segmento LAN mediante un protocolo *de paso de fichas,* que regula el tráfico transfiriendo un marco llamado *token* alrededor del anillo. Sólo se le permite transmitir al host que posea la ficha, eliminando así la colisión de paquetes. La arquitectura Token Ring negocia, en efecto, el tiempo de espera para las colisiones, porque cada estación debe esperar su turno antes de capturar la ficha para poder transmitir. No obstante, la eliminación de colisiones entre paquetes aumenta de manera significativa la utilización eficiente del ancho de banda de Token Ring. Algunas pruebas demuestran que Token Ring llega a utilizar hasta 75% de ancho de banda, comparado con el máximo teórico de Ethernet de casi 37%. El problema es que Token Ring sólo comienza a redituar arriba de ciertos volúmenes de tráfico.



Para persuadir al mercado de aceptar una nueva tecnología como un estándar *de facto* se requiere volumen. Token Ring es una gran tecnología, pero perdió la batalla frente a Ethernet en cuanto al número total de LAN instaladas. Desde el punto de vista del mercado, la necesidad de Token Ring de obtener grandes beneficios a partir de las LAN de gran tamaño tal vez resultó fatal. Casi todas las LAN son pequeñas porque gran parte de las compañías son pequeñas. Además, aún las grandes compañías tienen LAN de tamaño pequeño, ya sea en sucursales o en departamentos dentro de sus grandes edificios. Recuerde que estamos hablando de *segmentos* LAN en este contexto (el medio de transmisión compartido, no la "red local" que es una colección de todos los segmentos LAN conectados a la espina dorsal de la LAN).

Otro problema es que Token Ring requiere de elementos electrónicos muy costosos para que trabaje su proceso determinístico. Si lo piensa, es natural que la fabricación de una NIC que transmita paquetes "a voluntad" sea más económica que diseñar una que participe en un régimen ordenado en que sea necesaria una ficha. El costo es una de las razones primordiales por las que Token Ring perdió la batalla frente a Ethernet como el estándar más popular.

Cuando se presentó por primera vez Token Ring operaba a 4 Mbps, pero la mayor parte de las LAN se actualizaron a 16 Mbps. Si esto parece lento en comparación con las velocidades de 100 Mbps de Fast Ethernet, tenga presente que Token Ring ofrece mucho más ancho

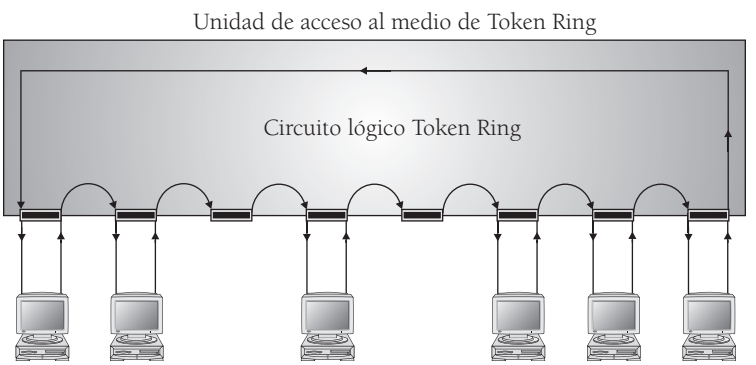


Figura 2-4. Las LAN Token Ring son anillos lógicos, no circuitos físicos reales.

de banda efectivo que la velocidad del cable. También se ofreció al público una especificación Token Ring a 100 Mbps, pero no se utilizó ampliamente.

ATM

ATM (modo de transferencia asincrónica) es una tecnología de red en el nivel de la vinculación de datos que, como Ethernet, Token Ring y FDDI, está especificada en la capa 2 del modelo OSI. Pero ahí es donde terminan las similitudes. ATM envía transmisiones por medio de celdas de 53 bytes en lugar de paquetes. Una *celda* es una unidad de mensaje de longitud fija. Como los paquetes, las celdas son porciones de un mensaje, pero el formato de longitud fija genera ciertas características:

- ▼ **Orientación de circuito virtual** Las redes que se basan en celdas operan mejor en modo punto a punto, en que la estación receptora está preparada para recibir y procesar activamente las celdas.
- ■ **Velocidad** El hardware sabe exactamente dónde termina el encabezado y empiezan los datos en cada celda, con lo que acelera las funciones de procesamiento. En la actualidad, las redes ATM funcionan a velocidades de hasta 40 Gbps.
- ▲ **Calidad de Servicio (QoS)** Las velocidades predecibles de transporte de datos y los circuitos virtuales permiten que las redes basadas en celdas garanticen de una manera más eficiente los niveles de servicio a los tipos de tráfico que tengan prioridad.

ATM no cuenta con una tecnología de control de acceso a medios. Es una tecnología de conmutación, en que se establece un circuito virtual antes de que comience la transmisión. Lo anterior difiere significativamente de las tecnologías LAN como Ethernet y Token Ring, que simplemente transmiten un mensaje sin una notificación previa al host receptor, dejando a los conmutadores y enrutadores que busquen la ruta más adecuada para llegar al destino.

Las celdas ATM son mucho más pequeñas que los paquetes de Ethernet. El tamaño de los paquetes de Ethernet puede variar desde 64 bytes hasta más de 1 500 bytes (hasta alrededor de 25 veces mayor por unidad de mensaje). Al ser mucho más granular, ATM se convierte en una tecnología más controlable.

ATM está diseñada para trabajar con cable de fibra óptica que opere la especificación SONET (red óptica sincrónica). SONET es un estándar ANSI que especifica las interfaces físicas que conectan el cable de fibra óptica a varias velocidades. Las especificaciones de SONET están especificadas para diferentes velocidades de cable llamadas *niveles de portador óptico*, u OC. A continuación se muestra una lista de las velocidades comúnmente utilizadas en el pasado y en la actualidad:

- ▼ **OC-1** Cable de fibra óptica a 52 Mbps.
- ■ **OC-3** Cable de fibra óptica a 155 Mbps.
- ■ **OC-12** Cable de fibra óptica a 622 Mbps.
- ■ **OC-24** Cable de fibra óptica a 1.2 Gbps.
- ■ **OC-48** Cable de fibra óptica a 2.5 Gbps.
- ■ **OC-96** Cable de fibra óptica a 4.9 Gbps.

- **OC-192** Cable de fibra óptica a 10 Gbps.
- **OC-256** Cable de fibra óptica a 13.27 Gbps.
- **OC-768** Cable de fibra óptica a 40 Gbps.

Como con las demás arquitecturas de paso de fichas, el diseño determinístico de ATM ofrece un gran ancho de banda efectivo a partir de la velocidad del cable. En realidad, se dice que el ancho de banda efectivo de ATM es superior a 75% de Token Ring. Casi todas las LAN de espina dorsal de ATM operan a velocidades OC-3 u OC-12. La mayor parte de los vínculos entre ciudades operan a OC-12, aunque los grandes proveedores de espinas dorsales para Internet están ofreciendo velocidades OC-48 y más elevadas para satisfacer las demandas de anchos de banda cada vez mayores.

Muchos consideran que ATM es la respuesta a la escasez de ancho de banda de Internet. Gran cantidad de empresas lo están instalando para reemplazar las espinas dorsales FDDI, que son muy costosas. ATM no sólo es rápido, sino que su comportamiento predecible se presta para garantizar la calidad de servicio (sobre todo en aplicaciones multimedia, que por su naturaleza no toleran latencia). Sin embargo, debido a la necesidad de adaptación de LANE (que es una técnica de encapsulamiento que fragmenta los paquetes de Ethernet o Token Ring en celdas ATM) ATM tiene un costo por puerto relativamente elevado. También introduce un nuevo protocolo en la mezcla, incrementando así su complejidad.

FDDI

FDDI son las siglas en inglés de interfaz de datos distribuidos por fibra, un protocolo a 100 Mbps que opera con cable de fibra óptica. De forma igual que Token Ring de IBM, FDDI utiliza la arquitectura de paso de fichas para controlar el acceso al medio de transmisión, brindando un ancho de banda efectivo muy elevado a partir de su velocidad de 100 Mbps. Si nunca ha escuchado hablar de FDDI, no es el único. FDDI ha tenido una exposición al público relativamente baja, porque se le ha utilizado tradicionalmente en espinas dorsales, no en LAN de acceso.

FDDI fue la tecnología estándar para redes espina dorsal

Durante muchos años, FDDI fue la tecnología de red favorita para LAN de espina dorsal. Esto podría atribuirse en parte a su velocidad. En la época en que se introdujo, FDDI fue la primera tecnología de red basada en fibra óptica, y su velocidad de 100 Mbps estableció el estándar.

Sin embargo, las LAN de espina dorsal siempre deben estar funcionando. Si la espina dorsal deja de trabajar, no puede haber interconectividad entre las LAN de acceso. Por esto, la especificación FDDI se diseñó de abajo arriba para garantizar disponibilidad, con una arquitectura física formada por dos anillos redundantes de fibra óptica. Cada estación se conecta a ambos anillos, lo que tiene dos efectos:

- La estación empezará a trabajar con el anillo de respaldo, en caso de que el anillo principal falle.
- La estación más cercana al punto de falla en el anillo principal funciona como conector para formar un circuito cerrado, convirtiéndose en un dispositivo que conecta el anillo y lo mantiene sin romperse.

NOTA Aunque cada estación debe estar conectada a ambos anillos para efectos de seguridad, en realidad sólo puede desplegarse un anillo.

La arquitectura FDDI proporciona redundancia de anillos duales

La arquitectura de FDDI la hace atractiva para su uso como LAN de espina dorsal, sobre todo en campus de oficinas y otras aplicaciones de gran cobertura. Los anillos duales proporcionan rutas redundantes. En operación normal, el anillo secundario permanece inactivo, transfiriendo sólo los marcos necesarios para mantenerse operando. El anillo secundario entra en acción cuando falla el principal. (Por lo general, las fallas son provocadas por una ruptura en la fibra o una NIC en estado de falla en algún punto de la red.) Como se muestra en la figura 2-5, FDDI aísla a la estación dañada conectándose al anillo secundario y haciendo un lazo en la dirección opuesta (por lo tanto, conservando el anillo intacto).

Debido a su diseño, una red FDDI puede tener configurado un cableado de fibra óptica de hasta 100 kilómetros (60 millas) de longitud (un rango al que suele considerarse una red de área metropolitana [MAN]). El alcance proviene del uso combinado del cableado de fibra óptica y el método de acceso a medios de paso de fichas (porque ambos soportan distancias mayores). Sin embargo, en realidad la mayor parte de las redes FDDI se localizan dentro de un edificio o campus de oficinas. Las pocas MAN que existen suelen pertenecer a compañías de energía eléctrica, que las usan para administrar desde un punto central sus redes de energía eléctrica. La tecnología FDDI se selecciona por sus características de seguridad contra fallas.

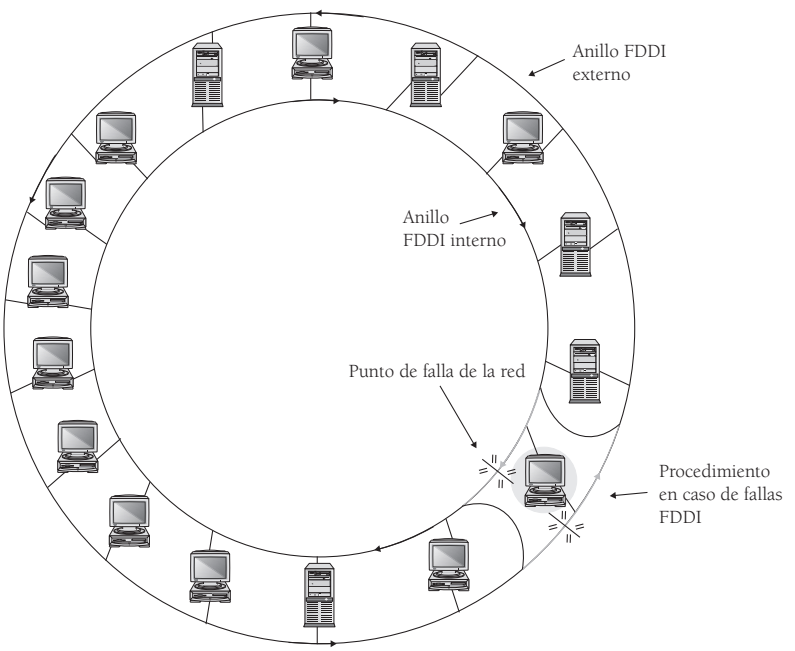


Figura 2-5. FDDI fue la espina dorsal predilecta por años, debido a su velocidad y redundancia.

FDDI puede trabajar ahora a través de cobre como CDDI

En un intento por expandir su aceptación en el mercado, FDDI se adaptó para trabajar sobre medios de par trenzado sin protección utilizando una tecnología llamada CDDI (interfaz de datos distribuidos por cobre). En realidad, CDDI es un nombre comercial, no un estándar, y Cisco adquirió la tecnología CDDI de Crescendo Communications en 1993. Aun con el visto bueno de Cisco, CDDI nunca tuvo éxito como una opción a las LAN de Ethernet. Después de una gran racha de popularidad como espina dorsal preferida de las grandes compañías conscientes de la confiabilidad, FDDI ha empezado a desaparecer de la escena, mientras ATM y Gigabit Ethernet toman su lugar como las tecnologías espina dorsal por excelencia.

Inalámbrico

En el campo de las LAN, una de las tecnologías más exitosas y útiles en años recientes ha sido el desarrollo y crecimiento de la conectividad inalámbrica. Al principio, los clientes podían conectarse a velocidades modestas de 11 Mbps. Sin embargo, con los avances recientes en tecnología, los clientes se pueden conectar a 54 Mbps y están en desarrollo velocidades todavía mayores.

Existe una gran variedad de estándares para la conectividad inalámbrica, incluidos los que son muy mencionados y que muchos tienen en sus casas: 802.11b y 802.11g (802.11a es menos común).

El primer estándar de LAN inalámbrica (WLAN) lo desarrolló en 1997 el Institute of Electrical and Electronics Engineers (IEEE). Era lento en comparación con los estándares actuales y funcionaba a una velocidad máxima de 2 Mbps. En realidad no tuvo éxito, por supuesto, de modo que en 1999 sacaron otro estándar que se conoce como 802.11b. Este estándar de uso común opera a 11 Mbps.

Mientras que trabajaba en el estándar 802.11b, el IEEE liberó también otra especificación llamada 802.11a. Este estándar opera en el rango de 5 Ghz del espectro inalámbrico, mientras que el 802.11b trabaja a 2.4 Ghz.

Debido a que trabaja a una frecuencia mayor, el 802.11a soporta velocidades de hasta 54 Mbps. El lado negativo es que las altas frecuencias tienden a ser más sensibles a obstáculos como muebles, pisos, paredes y hasta árboles. Así que la mayor velocidad debe compensarse con un menor alcance.

En estos últimos años, el (más) reciente estándar 802.11g finalmente fue puesto en marcha. En pocas palabras, es como el 802.11b pero más rápido. Opera en el rango de 2.4 Ghz del espectro inalámbrico, como el 802.11b, pero brinda velocidades de hasta 54 Mbps (algunos comercializadores han “extendido” el estándar para que soporte velocidades aún más elevadas). Como muchas personas habrán notado, el estándar 802.11g también soporta al 802.11b, si el equipo que se está conectando no soporta el nuevo estándar “g”.

LAN

Uno de los lugares más importantes donde la tecnología inalámbrica se puede observar es en un entorno LAN. Más allá de lo interesante de la tecnología inalámbrica (que es muy interesante), ésta permite la gran funcionalidad de poderse conectar sin tener que instalar cable Cat 5 por todos lados. Esto resulta útil en edificios viejos que seguramente no cuentan con techos suspendidos, o en cualquier otro lugar donde sería prohibitivo instalar cables.

La conectividad es posible por medio del uso de un adaptador inalámbrico en una computadora cliente y un *punto de acceso* (AP) conectado a un conmutador LAN. Las computadoras se comunican con la red utilizando la tarjeta inalámbrica para comunicarse con el AP.

WAN

La tecnología inalámbrica no está limitada sólo al mundo de las LAN. En realidad, las WAN inalámbricas se están convirtiendo en una gran opción en los negocios, sobre todo los que tienen edificios ubicados a pocos kilómetros de distancia.

Por ejemplo, mediante el uso de un par de puentes Aironet 1300 de Cisco y de antenas direccionales, se pueden conectar dos redes sin problema. No necesita solicitar ninguna licencia especial de radiodifusor y (aún mejor) no tiene que pagar una línea T1 o T3 privada.

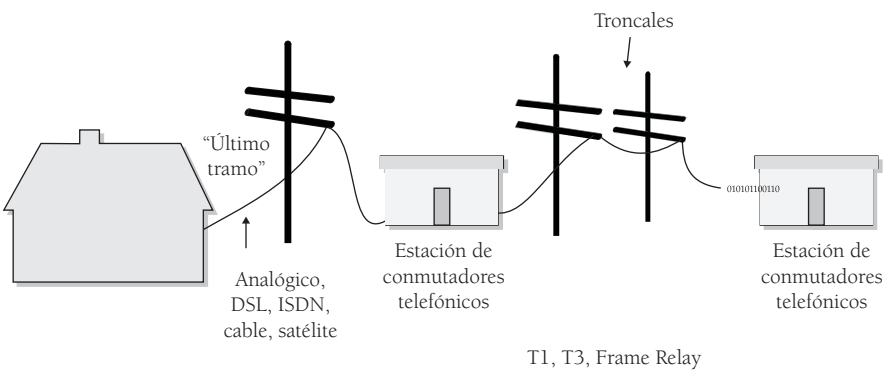
La interconectividad inalámbrica es un tema muy extenso (tanto que, de hecho, le hemos dedicado un capítulo completo). Consulte el capítulo 8 para conocer más información acerca de las tecnologías inalámbricas en general y de los productos inalámbricos de Cisco en particular.

TECNOLOGÍAS WAN

Casi todas las interconexiones tienen por lo menos algunos usuarios remotos. Las empresas necesitan conectar a las personas que trabajan en su casa y en oficinas remotas; los ISP necesitan tomar llamadas telefónicas de los suscriptores, etcétera. Existen dos tipos básicos de redes de área amplia (WAN):

- ▼ **De marcado telefónico** Una línea de marcado telefónico establece una conexión punto a punto entre un lugar central y uno o varios usuarios. Cuando la conexión ya no es necesaria, se libera el circuito telefónico.
- ▲ **Troncales** Una *troncal* es un vínculo punto a punto de alta capacidad entre oficinas. Por lo general, una troncal conecta a un gran número de usuarios remotos a un sitio central. Casi todas las troncales trabajan con líneas telefónicas T1 (a 1.5 Mbps) o T3 (a 45 Mbps), aunque están apareciendo en escena nuevas tecnologías (como ATM y Gigabit Ethernet).

Visto de otra forma, las redes telefónicas existen en dos planos: entre estaciones de conmutadores telefónicos y entre la estación de conmutadores y la casa o la oficina. Por supues-



to, la zona que se encuentra entre la estación de conmutadores vecina y la casa o el negocio es la más lenta, debido a su relativamente escasa infraestructura de telecomunicaciones.

En caso de que no lo sepa, las estaciones de conmutadores telefónicos son esos edificios pequeños y sin ventanas que suelen instalarse en ciertas áreas. Las estaciones de conmutadores de una ciudad son mucho más grandes y ocupan algunos pisos del edificio de la compañía telefónica local.

El último tramo de la interconexión se ha convertido en un campo de batalla clave entre los fabricantes de tecnología de interconectividad. Esto se debe a que, con el gran auge de Internet, cada vez son más las conexiones de marcado telefónico individuales que se conectan con sus ISP desde casa. Esto incluye a los empleados que trabajan en casa y que acceden a su información en la red corporativa, no sólo a la gente que navega por Web. Una gran batalla tecnológica ha surgido por el medio de transmisión del último tramo. Dicha contienda ha sido principalmente entre DSL e ISDN (dos tecnologías telefónicas digitales). Por arriba de estas tecnologías que utilizan el sistema telefónico público, los operadores de TV por cable y hasta las compañías satelitales se han unido para pasar por alto la red telefónica. En realidad, el cable de banda ancha le está quitando parte del negocio a las compañías telefónicas con servicios telefónicos caseros que operan con conexiones de banda ancha.

Tecnologías de marcado telefónico

Dos tecnologías han entrado al mercado para proporcionar ancho de banda digital a las casas y las oficinas pequeñas: ISDN y DSL. ISDN se introdujo en la década de 1980, pero los portadores telefónicos locales fueron un poco lentos para hacerla ampliamente disponible. Aunque no era lo que uno podría considerar como tecnología de marcado, DSL superó a ISDN al brindar mayores velocidades y más amplia disponibilidad.

Las tecnologías de marcado telefónico difieren de otras tecnologías WAN en que las conexiones que se establecen con ellas son temporales. En otras palabras, una vez que el usuario de la computadora ha terminado con la sesión, el circuito se libera al colgar el teléfono. Hasta el presente, casi todas las casas están conectadas por medio de circuitos telefónicos analógicos. Debido a que las líneas convencionales son analógicas, se necesitan módems en cada extremo; por esta razón algunos las conocen como circuitos *analógicos/módem.*

El principal problema con los circuitos analógicos/módem es que son lentos. Lo que los hace lentos es que las señales acústicas sólo utilizan una pequeña fracción del ancho de banda disponible en los cables de cobre del sistema telefónico, porque éstos fueron diseñados para voz y no para datos. Por ello, la conexión casera analógica más actual es a 56 Kbps (demasiado lenta, comparada con los 100 Mbps de Fast Ethernet, que es normal en los edificios de oficinas).

ISDN

ISDN, que son las siglas en inglés de red digital de servicios integrados, se propuso como el primer servicio digital para los hogares. La mejora primordial de éste sobre la líneas analógicas/módem es que los circuitos ISDN son digitales, y por eso utilizan el denominado CPE (equipo en las instalaciones del usuario) en lugar de módems (CPE es una término telefónico clásico).

ISDN crea varios canales en una sola línea. Un *canal* es una ruta de datos multiplexada en un solo medio de comunicación. (*Multiplexar* significa combinar varias señales en una

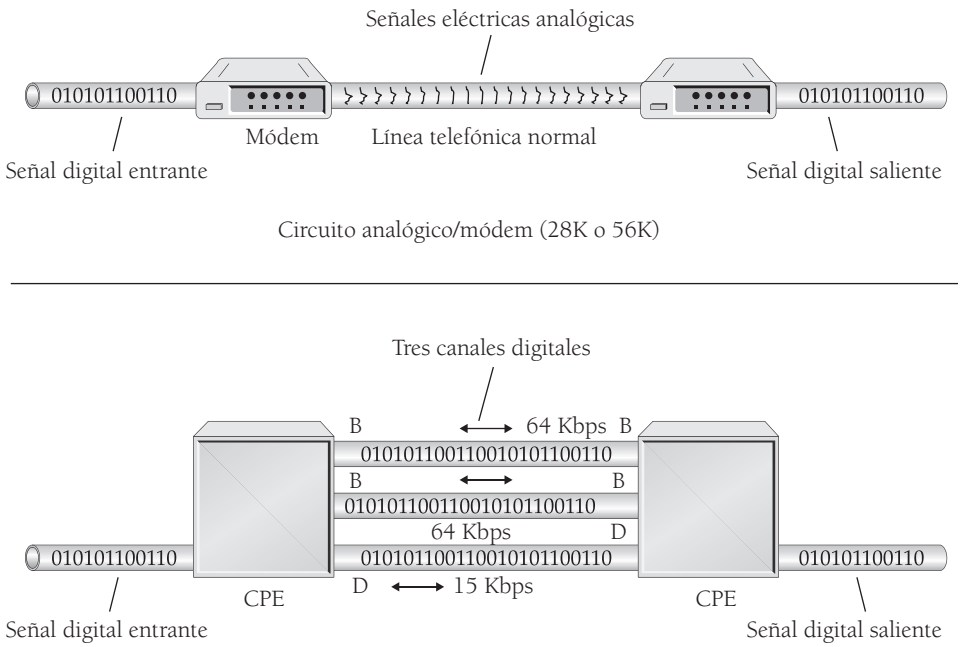


Figura 2-6. Un circuito BRI de ISDN lleva tres canales digitales a una casa u oficina.

sola línea.) El circuito básico en ISDN es el BRI (interfaz a velocidad básica) que está formado por los famosos canales *B*, o del cliente, para transportar información. En la figura 2-6 se muestra un contraste entre un circuito analógico/módem y uno BRI de ISDN.

Cada canal B opera a 64 Kbps hasta un total de 128 Kbps de ancho de banda útil. Al tener canales B separados se mejora el transporte de datos en conexiones simétricas (en otras palabras, sesiones caracterizadas por el flujo de tráfico bidireccional y simultáneo). Un tercer canal, llamado canal *D* (o delta) transporta 16 Kbps. El canal D está dedicado al control de la red en lugar de información útil. Al manejar el control del envío de la información por separado, se mejora el desempeño y la confiabilidad de ISDN.

Un segundo tipo de circuito ISDN es uno PRI (interfaz de velocidad primaria). El PRI es básicamente lo mismo que el BRI, excepto que empaqueta hasta 23 canales B, más un canal D de 64 Kbps, ocupando un ancho de banda útil de hasta 1 544 Mbps. Los negocios pequeños utilizan circuitos PRI para conectar a varios usuarios, compitiendo por el extremo inferior del nicho tradicional del mercado de T1.

DSL

DSL son las siglas en inglés de línea de suscriptor digital. Como su nombre lo indica, DSL también transporta señales digitales a través de alambre de cobre. Utiliza algoritmos complejos para modular señales de tal forma que puede exprimir más ancho de banda de la infraestructura existente en el último tramo.

DSL es una tecnología de telecomunicaciones inherentemente asimétrica. Lo que esto significa es que los datos pueden transferirse más rápido hacia abajo (de la central telefónica local hacia su casa) que en la otra dirección. Existen varios tipos de DSL; dos son importantes en nuestro análisis:

- ▼ **aDSL** El DSL asimétrico, un circuito bidireccional que maneja alrededor de 640 Kbps hacia arriba y hasta 6 Mbps hacia abajo.
- ▲ **DSL Lite** También conocida como G.Lite, es una tecnología más económica que puede transportar datos a velocidades entre 1.5 Mbps y 6 Mbps aproximadamente hacia abajo y de entre 128 Kbps y 384 Kbps hacia arriba. Las velocidades exactas dependen del equipo que se instale y de la distancia a la central telefónica.

La asimetría inherente de DSL se adapta perfectamente a Internet, donde la mayoría de los usuarios de pequeña oficina y oficina en casa descargan más información de la que suben a la red de Internet.

El factor clave que se debe conocer es que DSL requiere una pieza especial de equipo llamada módem DSL para funcionar. El módem DSL es el que divide las señales en canales hacia arriba y hacia abajo. La diferencia principal con DSL Lite es que la división de las señales se lleva a cabo en la central telefónica y no en la casa o la pequeña oficina. En la figura 2-7 se muestra lo anterior.

Al no requerir la división de la señal DSL en casa hace que DSL sea mucho más factible económicamente que ISDN. Para utilizar más circuitos DSL, no debe estar ubicado más allá de seis Outlook ocho kilómetros de la central de conmutador telefónico.

Conexiones de módem por cable y satelitales

Dos formas adicionales de obtener acceso de marcado se encuentran en la parte trasera de su televisor, representadas por el cable coaxial. Los módems por cable y las conexiones satelitales están adquiriendo popularidad como formas de acceder a Internet a altas velocidades.

Módem por cable Un módem por cable se conecta a un alimentador existente de televisión por cable y a una tarjeta de red Ethernet en la computadora. A pesar de que los módems por cable y los de marcado telefónica brindan acceso a la red y se conocen como "módems", son dispositivos muy diferentes. Mientras que ambos realizan su trabajo de forma muy distinta, la mayoría de los usuarios reconocerían esta diferencia principalmente por la velocidad. Los módems de marcación telefónica de mejor calidad proporcionan una velocidad de 56 Kbps a través del servicio telefónico convencional. Las velocidades que alcanzan los módems por cable se encuentran en el rango de 384 Kbps a varios millones de bits por segundo, dependiendo del proveedor del servicio y del paquete adquirido.

Cuando los módems por cable aparecieron, no había estándares y los aparatos de diferentes marcas no podían comunicarse entre sí. Sin embargo, la industria finalmente generó el estándar especificación de la interfaz para el servicio de Datos a través de cable (DOCSIS). Esto permitió que los comercializadores diseñaran módems de cable que cumplieran con este estándar, lo que dio como resultado costos más accesibles para el equipo.

Conexión satelital Si el cable o DSL no son opciones y aún siente la necesidad de disponer de más velocidad, basta con que busque más allá de las nubes. Las conexiones satelitales son ideales para los que desean acceso a alta velocidad a la red, pero se encuentran ubicados en lugares donde no se da servicio por cable o DSL.

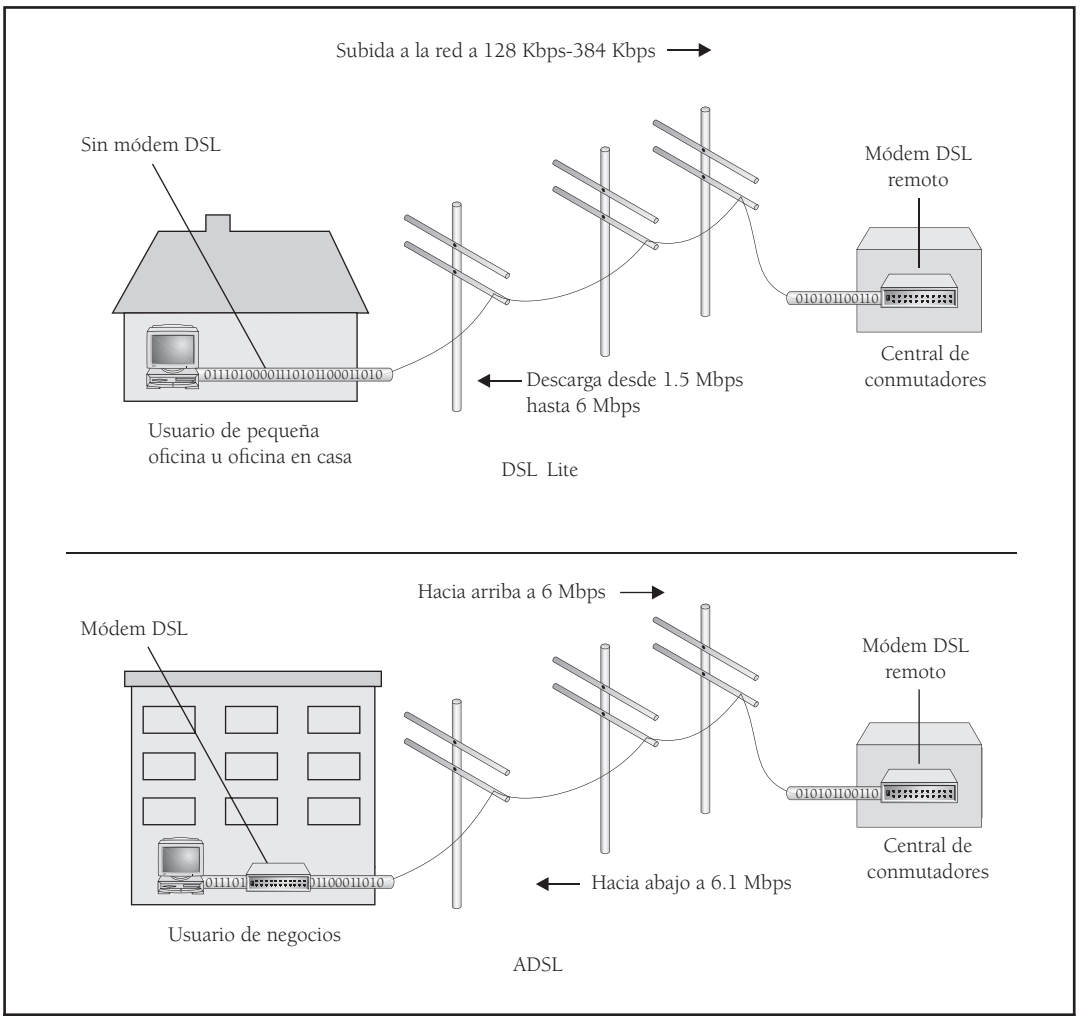


Figura 2-7. Los módems DSL dividen el tráfico en dos canales direccionales para lograr un ancho de banda alta.

Compañías como Hughes Network Systems ofrecen entrega satelital de contenido de Internet. De manera muy parecida a las antenas de 18 pulgadas atornilladas a las paredes y los techos de millones de casas que se utilizan para la televisión digital y cine, estos servicios utilizan transmisiones de gran ancho de banda para ofrecer acceso de alta velocidad a Internet.

Tecnologías troncales WAN

Como ya se mencionó, una troncal es un vínculo de datos punto a punto a alta velocidad. Las troncales pueden encontrarse dentro de edificios y campus de oficinas, pero son mejor conocidas como vínculos de área amplia entre edificios, ciudades, regiones y aun entre continentes.

La tecnología WAN ha evolucionado notablemente en la última década y no sólo con la expansión de Internet. Por ejemplo, la tecnología de conmutación de paquetes Frame Relay probó ser mucho más económica que las líneas WAN privadas dedicadas. Analizaremos brevemente las tecnologías WAN en uso. Todas ellas comparten características comunes en el sentido de que son circuitos dedicados (y no de marcado telefónico y colgado), con gran ancho de banda utilizadas para conectar sitios con muchos usuarios, en contraste con sitios de oficina pequeña y oficina en casa con uno o dos usuarios.

Casi todas las empresas están reemplazando los servicios de WAN de línea arrendada con servicios de infraestructura compartida. Su principal motivación es ahorrar dinero, pero la flexibilidad también representa un gran beneficio.

Líneas privadas T1 y T3

T1 y T3 son las tecnologías de línea arrendada predominantes en Norteamérica y Japón. (Existen equivalentes en Europa llamados E1 y E3.) Un circuito (o parte de un circuito) de línea arrendada está reservado para la compañía que lo renta (y se paga a una tarifa mensual específica, sin importar la cantidad de tiempo que se utilice).

T1 utiliza una tecnología de telecomunicaciones llamada *multiplexión por división de tiempo (TDM)* para proporcionar una velocidad de datos de casi 1.5 Mbps. TDM combina flujos de datos al asignar a cada flujo una ranura de tiempo diferente en un conjunto y transmitir de manera repetida una secuencia fija de ranuras de tiempo por un único canal de transmisión. Las líneas T1 utilizan alambre de cobre, dentro y entre áreas metropolitanas. Puede comprar un circuito T1 a su compañía telefónica local o rentar una parte de su ancho de banda en un arreglo llamado *T1 fraccionado*. Algunos ISP están conectados a Internet mediante circuitos T1.

T3 es una opción más rápida que T1. Los circuitos T3 son conexiones telefónicas dedicadas que transportan datos a 45 Mbps. Las líneas T3 las utilizan principalmente *ISP de primer nivel* (ISP que conectan a Internet a otros ISP de menor tamaño) y grandes empresas. Debido a su gran ancho de banda y a su costo, casi todas las líneas T3 son rentadas como líneas T3 fraccionadas. A las líneas T3 también se les conoce como líneas *DS3*.

Frame Relay

Frame Relay conmuta paquetes en una red compartida de conmutación de paquetes que es propiedad de una portadora, como una compañía telefónica regional. Como se muestra en la figura 2-8, Frame Relay utiliza circuitos telefónicos locales para vincular lugares remotos. Las conexiones de larga distancia se llevan a cabo a través de la infraestructura de telecomunicaciones que es propiedad del proveedor del servicio de Frame Relay y compartida entre muchos otros clientes.

NOTA En este contexto, cuando decimos que Frame Relay *conmuta* paquetes, la conmutación es una tecnología diferente de la usada por los conmutadores LAN.

El beneficio principal de Frame Relay es la comparación entre costo y eficiencia. Frame Relay toma su nombre del hecho de que coloca datos en unidades de mensaje de tamaño variable llamadas marcos (frames). Deja la administración de sesiones y la corrección de errores a los nodos que opera en varios puntos de conexión, lo que acelera el desempeño de la red. Casi todos los clientes de Frame Relay rentan *circuitos virtuales permanentes*, o *PVC*. Un PVC

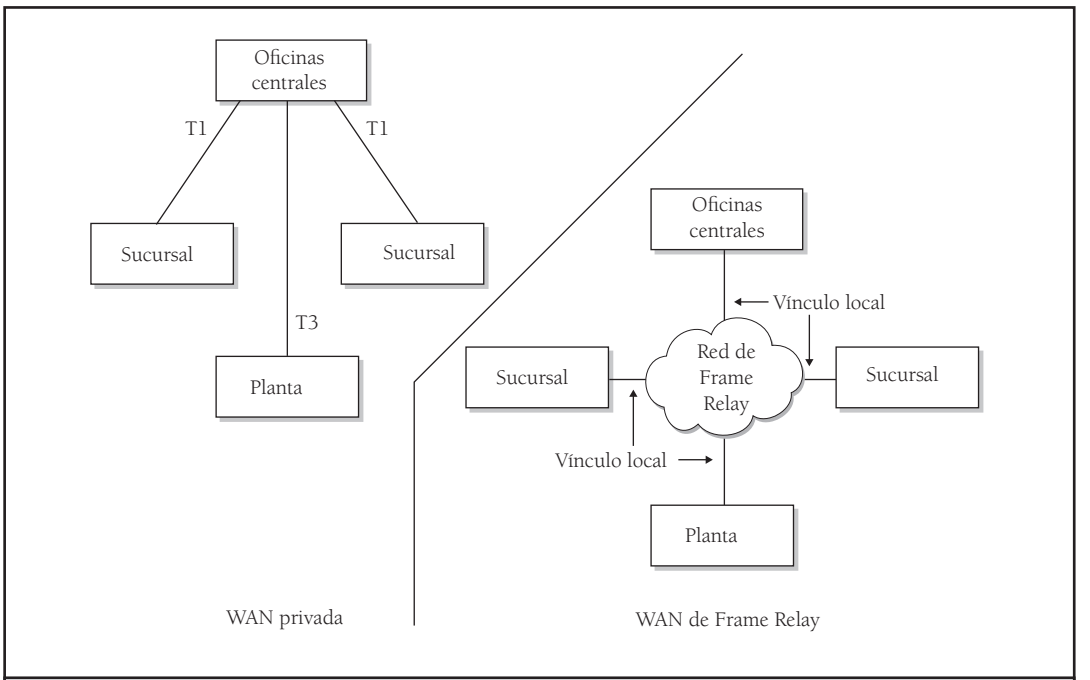


Figura 2-8. Frame Relay puede ser un enlace WAN eficiente para tráfico intermitente.

proporciona al cliente una conexión continua y dedicada sin tener que pagar por la línea arrendada, que utiliza circuitos permanentes dedicados. A los clientes de Frame Relay se les cobra de acuerdo con el nivel de uso. También tienen la opción de seleccionar entre niveles de servicio, donde la calidad del servicio se programa de acuerdo con la prioridad que se les otorga a los marcos del cliente dentro de la nube de Frame Relay.

Las redes de Frame Relay se encuentran por arriba de las troncales T1 o T3 administradas por el operador de red de Frame Relay. El uso de Frame Relay tiene sentido económico cuando el tráfico no es lo suficientemente considerable como para que se requiera una conexión ATM dedicada.

VPN

Las VPN (redes privadas virtuales) son interconexiones empresariales operadas en Internet. Las VPN trabajan utilizando una técnica de cifrado para formar un "túnel" a lo largo de una determinada ruta de red para llegar a sitios remotos. El *cifrado* es la técnica de desordenar los datos para que la estación receptora con la llave apropiada pueda descifrarlos, leerlos. Se aplican también otras técnicas para asegurarse que la integridad de los datos esté intacta (es decir, que el contenido quede en su lugar y no se haya alterado) después de que un mensaje ha recorrido un túnel VPN. En la figura 2-9 se muestra cómo una empresa puede utilizar una VPN para interconectar sus sitios.

Un escenario típico de VPN se presenta cuando una empresa acude con un ISP de nivel 1 y compra una conexión de red en cada sitio remoto.

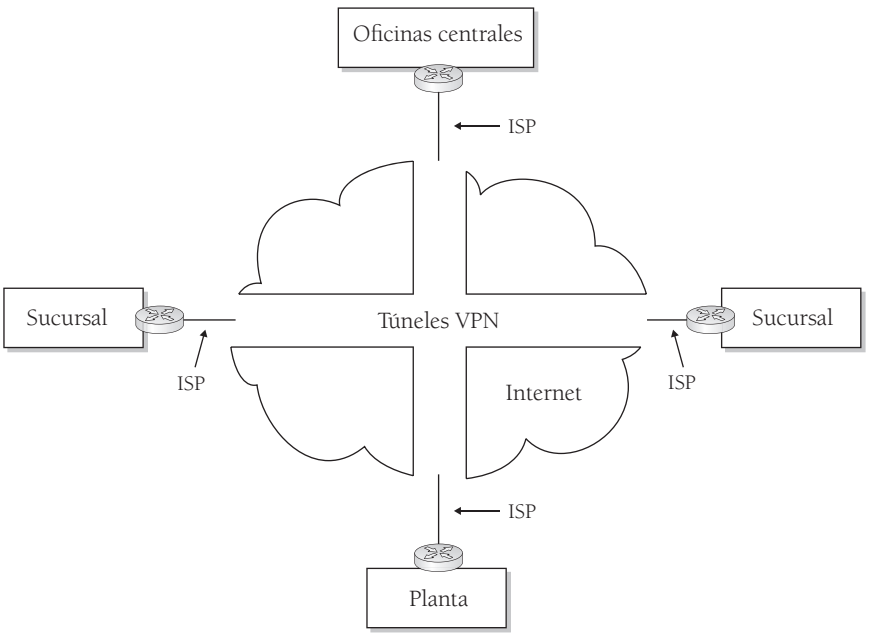


Figura 2-9. Las VPN se basan en túneles y cifrado para trabajar en la infraestructura de Internet.

Los enrutadores deben configurarse en cada oficina de la compañía para realizar las operaciones de cifrado y descifrado. Esto es mucho más fácil de hacer ahora que hace algunos años, porque existen muchas aplicaciones de software que ayudan a configurar un túnel VPN.

TCP/IP

Internet trabaja con TCP/IP, el protocolo de control para la transmisión/protocolo Internet. TCP/IP es, en realidad, un conjunto de protocolos, cada uno de los cuales lleva a cabo un papel específico para permitir que las computadoras hablen el mismo idioma. TCP/IP es un protocolo universalmente aceptado y es casi seguro que se use en las computadoras con las que trabaja en casa y la oficina. Esto es cierto, sin considerar los protocolos LAN, porque los proveedores de LAN han implementado la compatibilidad TCP/IP en sus productos. Por ejemplo, el último producto NetWare de Novell trabaja con el protocolo TCP/IP.

TCP/IP fue diseñado por la Defense Advanced Research Projects Agency (DARPA), en la década de 1970 (con la idea de permitir que computadoras de diferentes marcas se comunicaran sin problemas y sin importar su ubicación). En los primeros días, se trabajo con TCP/IP en computadoras UNIX, lo que contribuyó a la popularidad del protocolo a medida que los proveedores adoptaron la práctica de incluir software TCP/IP dentro de

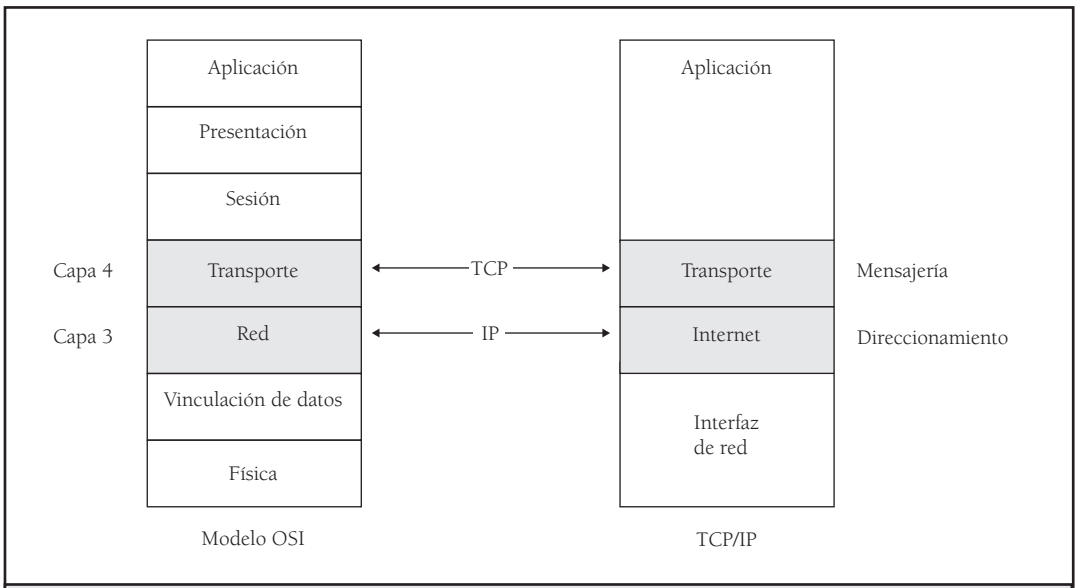


Figura 2-10. La pila de protocolos TCP/IP cumple con el modelo de referencia de las siete capas.

cada computadora UNIX. Como tecnología, TCP/IP tiene la correspondencia con el modelo de referencia OSI que se muestra en la figura 2-10.

Al observar la figura 2-10, notará que TCP/IP se concentra en las capas 3 y 4 del modelo de referencia OSI. La teoría es dejar las tecnologías de red a los proveedores LAN. El objetivo de TCP/IP es transferir mensajes a través de casi cualquier producto LAN para establecer una conexión que ejecute casi cualquier aplicación de red.

El protocolo TCP/IP funciona porque se equipara de cerca con el modelo OSI en los dos niveles inferiores (las capas física y de vinculación de datos). Lo anterior permite que TCP/IP se comunique casi con cualquier tecnología de red y, de forma indirecta, con cualquier tipo de plataforma de cómputo. Las cuatro capas abstractas de TCP/IP son las siguientes:

- ▼ **Interfaz de red** Permite que TCP/IP interactúe con todas las tecnologías modernas de red, porque cumple con el modelo OSI.
- ■ **Internet** Define la forma como IP envía mensajes mediante enrutadores a través de interconexiones como Internet.
- ■ **Transporte** Define el mecanismo de intercambio de mensajes entre computadoras.
- ▲ **Aplicación** Define las aplicaciones de red que habrán de realizar tareas como transferencia de archivos, correo electrónico y otras funciones útiles.

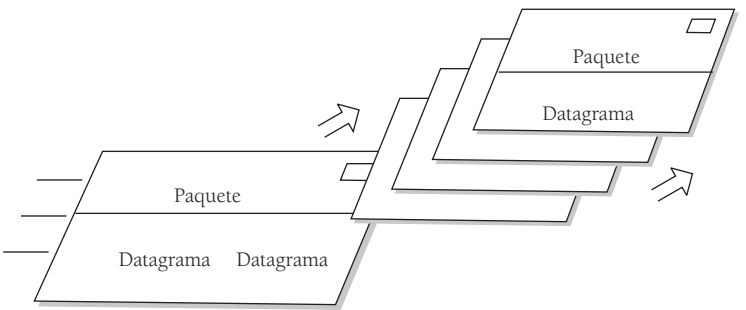
TCP/IP es el estándar *de facto* que unifica Internet. Una computadora que implemente una tecnología de red de una capa del modelo OSI, como Ethernet o Token Ring, ha superado las incompatibilidades que de otra forma existirían entre plataformas como Windows, UNIX, MAC, mainframes IBM y otras. Ya hemos estudiado las capas 1 y 2 en nuestro análi-

sis de las tecnologías LAN que conectan grupos de computadoras en un determinado sitio. Ahora estudiaremos cómo se interconectan las computadoras en Internet o interconexiones privadas.

Mensajería TCP/IP

Todos los datos que se transfieren en una red deben tener un formato para que los dispositivos sepan cómo manejarlos. La capa de Internet de TCP/IP (que se correlaciona con la capa de red del modelo OSI) está basada en un formato fijo de mensaje que se llama *datagrama IP* (el contenedor que incluye la información que integra el mensaje). Por ejemplo, cuando descarga una página Web, lo que ve en la pantalla se entregó dentro de datagramas.

Muy relacionado con el datagrama está el paquete. Mientras que un *datagrama* es una unidad de datos, un *paquete* es una entidad física que consta de una unidad de mensaje que pasa por la interconexión. A menudo, la gente utiliza los términos de forma intercambiable; la diferencia sólo es importante en ciertos contextos cerrados. Lo importante es que casi todos los mensajes se envían en fragmentos y se reensamblan en el extremo receptor.



Flujo del paquete

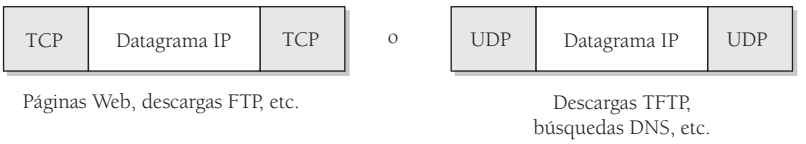
Por ejemplo, cuando envía a alguien un correo electrónico, éste recorre el alambre como un flujo de paquetes. Un correo electrónico pequeño puede estar formado por sólo diez paquetes; uno grande puede dividirse en miles. En el extremo opuesto, un mensaje de solicitud de servicio podría ocupar tan sólo un paquete.

Una ventaja de este método es que si un paquete se corrompe durante la transmisión, sólo es necesario reenviar ese paquete, no todo el mensaje. Otra ventaja es que a ningún host se le obliga a esperar un enorme periodo a que termine la transmisión de otro host, para que pueda transmitir su propio mensaje.

Comparación entre TCP y UDP como protocolos de transporte

Un mensaje IP se envía utilizando uno de dos protocolos de transporte: TCP o UDP. TCP son las siglas en inglés de protocolo de control para la transmisión; UDP, las de protocolo de datagrama de usuario, y se utiliza en lugar de TCP en mensajes de menor importancia. Cualquiera de los dos protocolos proporciona los servicios de transporte necesarios para guiar los mensajes a través de las interconexiones TCP/IP. TCP es un protocolo *confiable* porque verifica con el receptor para asegurarse de que se haya recibido el paquete, enviando un mensaje ACK (reconocimiento) cuando ha finalizado la transmisión. UDP es un protocolo *no confiable* o *sin conexión*, porque no se lleva a cabo ninguna acción encaminada

a confirmar la entrega del mensaje. Ambas tecnologías de transporte operan en la capa 4 de la arquitectura OSI.



No deje que el nombre TCP/IP lo confunda. TCP no forma parte de un mensaje UDP. Y mientras estamos en eso, tampoco deje que el nombre protocolo de datagrama de usuario lo confunda. Un mensaje IP que se envía por medio de TCP contiene un datagrama IP de la misma forma que un mensaje UDP también lo contiene.

Un aspecto que resulta importante es que sólo puede utilizarse un protocolo de transporte para manejar un mensaje. Por ejemplo, cuando descarga una página Web, los paquetes son manipulados por el protocolo TCP sin que UDP tenga participación alguna. Por el contrario, la carga o descarga mediante un protocolo trivial de transferencia de archivos (TFTP) es manejada totalmente por el protocolo UDP.

El protocolo de transporte que habrá de utilizarse depende de la aplicación de red (correo electrónico, descarga de páginas Web HTTP, administración de red, etcétera). Como se estudiará después, los diseñadores de software para redes utilizarán el UDP siempre que sea posible, porque éste genera menos sobrecarga de tráfico. TCP se extiende a distancias más grandes para asegurar la entrega y envía más paquetes que el UDP para manejar las conexiones. En la figura 2-11 se observa una muestra de aplicaciones de red para ilustrar la división entre los protocolos de transporte TCP y UDP.

Los ejemplos de la figura 2-11 destacan algunos aspectos importantes. En primer lugar, FTP y TFTP llevan a cabo, en esencia, la misma tarea (manejar la transferencia de archivos

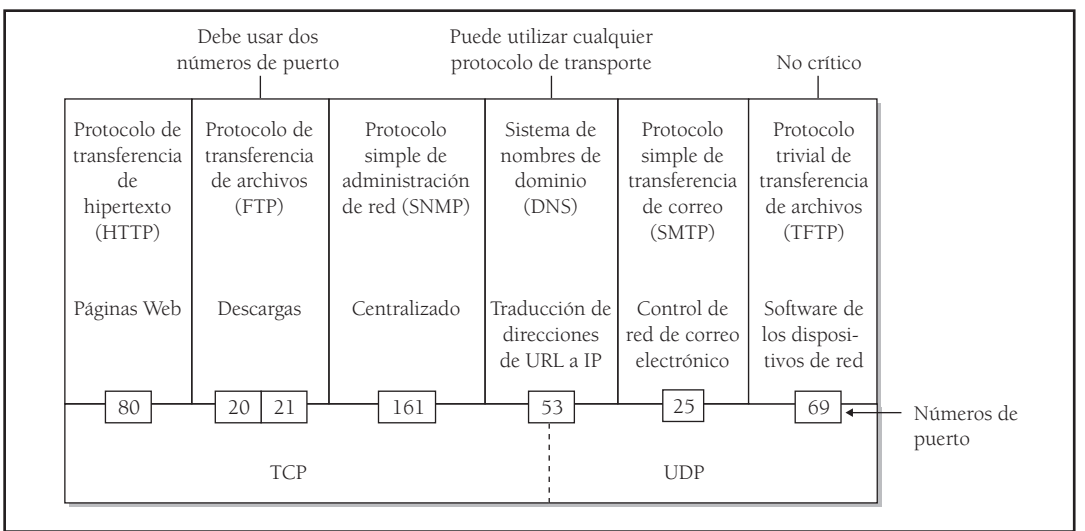


Figura 2-11. Los protocolos TCP y UDP manejan diferentes aplicaciones de red (números de puerto).

de datos). La principal diferencia es que TFTP se utiliza, en esencia, para descargar y respaldar el software de los dispositivos de red, y utiliza UDP porque la falla de dicho mensaje es tolerable (la información útil de TFTP no es para usuarios finales, sino para administradores de red, quienes tienen prioridad baja). El sistema de nombres de dominio (DNS), el servicio que traduce las direcciones URL a IP, utiliza UDP para búsquedas de nombre de cliente a servidor y TCP para búsquedas de servidor a servidor. Sin embargo, tal vez sólo se emplee uno de los dos para una conexión particular de búsqueda DNS.

Formato del datagrama IP

El datagrama es la unidad básica de datos dentro de los paquetes IP. El formato de datagrama proporciona campos para el manejo de mensajes y para los datos útiles. En la figura 2-12 se muestra el esquema de un datagrama. No se confunda por las proporciones de los campos de la figura; el campo de datos es el más grande en casi todos los paquetes.

Las computadoras se conectan. Los paquetes que llevan a cabo la conexión contienen la dirección IP del remitente y las direcciones de destino. Además, contienen información adicional como una instrucción para descargar una página Web. Los otros 12 campos de los paquetes tienen propósitos administrativos.

Un factor clave acerca de los paquetes IP es que tienen una longitud variable. Por ejemplo, en las LAN de Ethernet, un paquete puede tener 200 bytes de longitud, otro 1,400 bytes. Los paquetes IP pueden llegar a tener una longitud de 4 000 bytes en los paquetes Token Ring.

NOTA En este contexto, hablamos de bytes en lugar de bits porque los datagramas contienen datos y las computadoras prefieren manejar bytes. Por otro lado, cuando se estudian los flujos de tráfico, digamos, a través de un cable, la unidad de medida son los bits (la unidad preferida en el ambiente de las redes).

Un paquete tiene dos partes básicas: la información del encabezado y los datos. La parte de los datos del paquete contiene la carga (la información útil que se está enviando por la

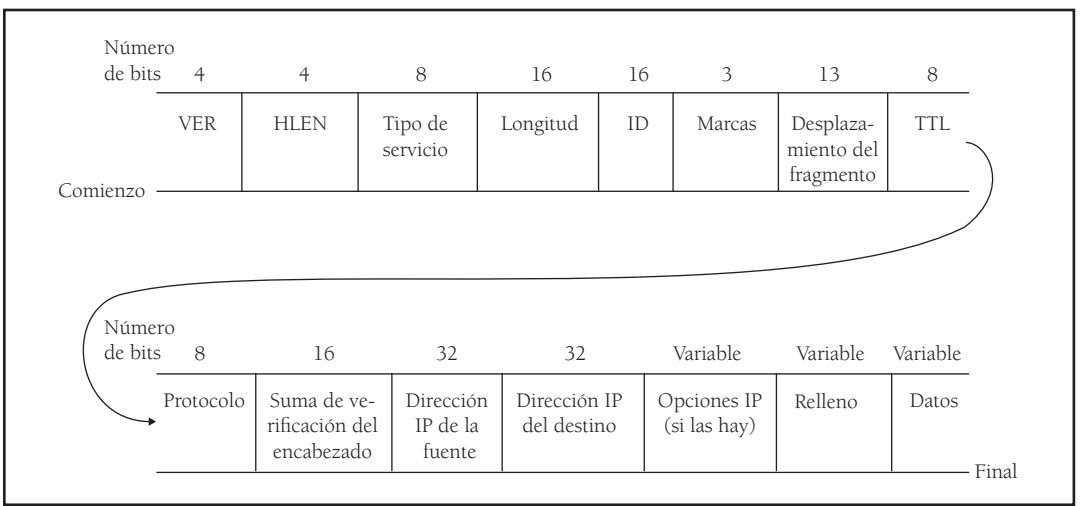


Figura 2-12. El formato del datagrama IP tiene longitud variable.

red). El encabezado contiene la información de control necesaria para que los enrutadores y las computadoras manejen el paquete y lo coloquen en orden con respecto a los demás paquetes que integran el mensaje completo.

Tenga siempre presente que la CPU que maneja el paquete necesita conocer la posición exacta del bit donde comienza cada campo; de otra manera, todo sería sólo una cadena de ceros y unos sin ningún sentido. Tome en cuenta que los tres campos que pueden tener longitud variable se colocan en el lado derecho del formato. Si los campos de longitud variable estuvieran a la izquierda, sería imposible que las computadoras supieran dónde empiezan los campos subsecuentes. Los campos de un datagrama IP son los siguientes:

- ▼ **VER** La versión de IP utilizada por la estación que originó el mensaje. La versión actual es la 4. Este campo permite que diferentes versiones coexistan en una interconexión.
- ■ **HLEN** Significa *longitud del encabezado* y le informa al receptor el tamaño del encabezado, para que la CPU sepa dónde comienza el campo de datos.
- ■ **Tipo de servicio** Es un código que indica al enrutador cómo se deberá manejar el paquete en términos de nivel de servicio (confiabilidad, precedencia, retardo, etcétera).
- ■ **Longitud** Es el número total de bytes en todo el paquete, incluidos todos los campos, el encabezado y los datos.
- ■ **ID, marcas y desplazamiento de fragmentos** Estos campos indican al enrutador cómo fragmentar y reensamblar los paquetes y cómo desplazar diferentes tamaños de marco que podrían encontrarse a medida que los paquetes viajan por los distintos segmentos LAN utilizando diferentes tecnologías de red (Ethernet, FDDI, etcétera).
- ■ **TTL** Son las siglas en inglés de tiempo de vida; se trata de un número que disminuye uno cada vez que se envía un paquete. Cuando el contador llega a cero, se elimina el paquete. TTL evita que ciclos en el enrutador y paquetes perdidos vaguen interminablemente por interconexiones.
- ■ **Protocolo** El protocolo de transporte que debe utilizarse para manejar el paquete. Este campo casi siempre identifica TCP como protocolo de transporte, pero pueden utilizarse otras formas de transporte para manejar los paquetes IP.
- ■ **Suma de verificación del encabezado** Una *suma de verificación* es un valor numérico utilizado para asegurar la integridad del mensaje. Si las sumas de todos los paquetes del mensaje no llegan al valor correcto, la estación sabe que el mensaje fue alterado.
- ■ **Dirección IP de la fuente** La dirección de 32 bits del host que originó el mensaje (por lo general una PC o un servidor).
- ■ **Dirección IP destino** La dirección de 32 bits del host al que se está enviando el mensaje (por lo general una PC o un servidor).
- ■ **Opciones IP** Se utiliza para efectuar pruebas en la red y para otros propósitos especiales.
- ■ **Relleno** Rellena cualquier posición de bit no utilizada, para que la CPU pueda identificar correctamente la primera posición de bit del campo de datos.
- ▲ **Datos** La información útil que se envía. Por ejemplo, un campo de datos del paquete puede contener parte del texto que conforma un mensaje de correo electrónico.

Números de puerto

Un número de puerto identifica la aplicación de red ante las capas superiores de la pila de protocolos. Por ejemplo, cada paquete en una transmisión de correo electrónico contiene el número de puerto 25 en su encabezado, para indicar que se está utilizando la aplicación de protocolo de transferencia de correo simple (SMTP). Existen cientos de números de puerto asignados. La Internet Assigned Numbers Authority (IANA) coordina las asignaciones de números de puerto, de acuerdo con el sistema siguiente:

- ▼ **Número 1023 e inferiores** Puertos "bien conocidos", asignados a aplicaciones públicas (como SMTP) y a compañías para identificar productos para aplicaciones de red.
- ■ **Números 1024 a 49151** Números reservados, registrados y asignados para su uso por parte de compañías específicas.
- ▲ **Números 49152 a 65535** Números asignados de manera dinámica por la aplicación del usuario final que utiliza la aplicación de red.

Los números de puerto ayudan a las estaciones a mantener un registro de las diferentes conexiones que se procesan de manera simultánea. Por ejemplo, por razones de seguridad, casi todos los firewalls se configuran para leer los números de puerto en el encabezado de cada paquete.

Muchos principiantes se confunden con la manera en que se utilizan exactamente los números de puerto. Por ejemplo, si trata de conectarse a un servidor Web desde su PC, tal vez crea que ambas estaciones terminales utilizarán el puerto 80 (HTTP) para realizar la descarga de una página Web. En realidad, el cliente solicitante utiliza un número de puerto aleatorio en el campo del puerto de origen del paquete de solicitud y sólo utiliza el puerto HTTP asignado número 80 en el campo de puerto de destino. En la figura 2-13 se muestra cómo se utilizan los números de puerto durante una transmisión.

El cliente utiliza un número de puerto aleatorio como ayuda para mantener un registro de las conversaciones que se presentan durante una conexión. Una *conversación* es una transacción discreta puerto a puerto entre dos estaciones terminales. Puede presentarse cualquier número de conversaciones dentro de una sola conexión.

Al observar la figura 2-13, es probable que la página que se descargó en el paso 2 haya incluido uno de los molestos comandos HTML que automáticamente crean una nueva ventana de navegación sin que lo haya solicitado (un *pop-up* o ventana emergente). La ventana emergente solicita que se descargue una nueva página, creando así toda una nueva ráfaga de código HTML, texto, GIF y JPEG que es necesario manejar (en otras palabras, una segunda conversación).

Sin embargo, en el extremo del servidor, debe utilizarse un número de puerto reconocido ampliamente, como el 80 para HTTP (de otra forma, los miles de anfitriones que accedan al servidor Web no tendrán idea de qué aplicación pedir).

La capa de transporte

La forma en que se manejan los paquetes difiere dependiendo del tipo de tráfico. Existen dos técnicas para el envío de paquetes mediante una interconexión TCP/IP: orientada a la conexión y sin conexión. Por supuesto que, en estricto sentido, se establece una conexión siempre que un paquete alcanza su destino. *Orientado a la conexión y sin conexión* alude al nivel de esfuerzo y control que se aplica para manejar un mensaje.

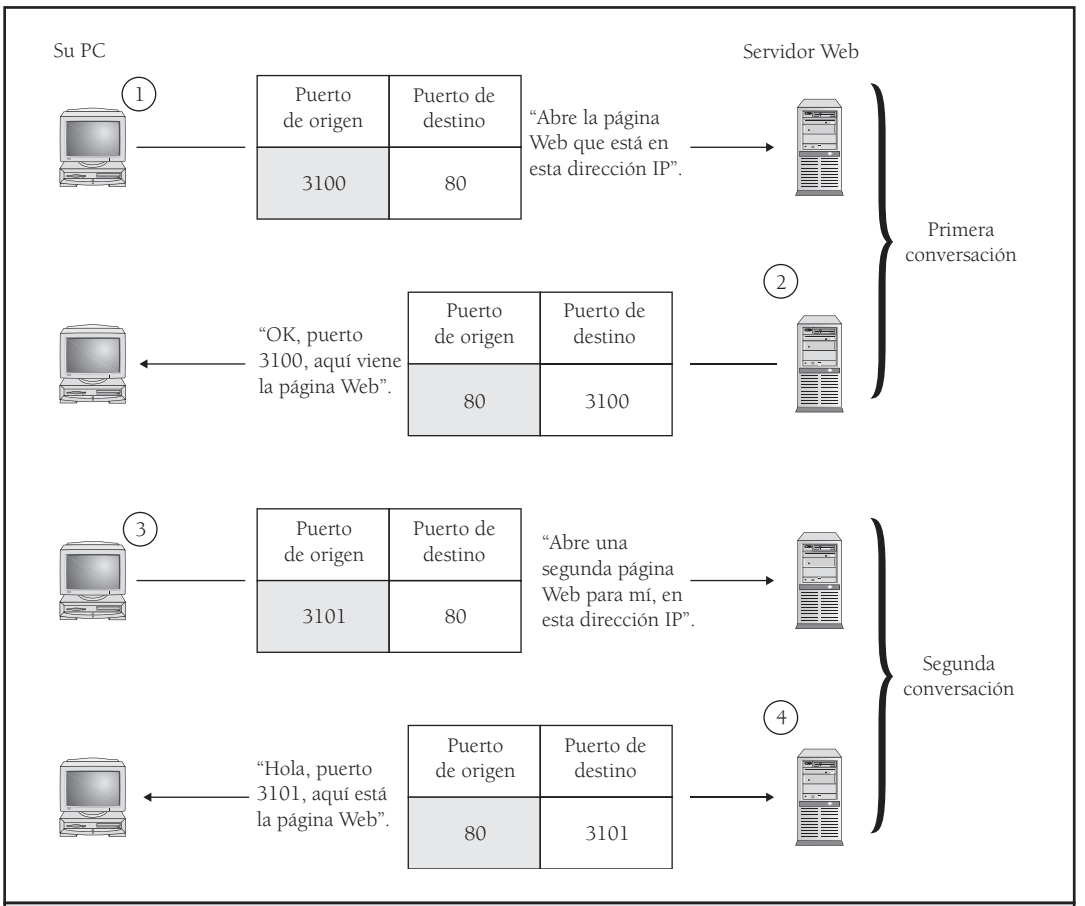


Figura 2-13. Los números de puerto identifican la aplicación de red que está utilizando el mensaje.

Cada paquete que circula por una interconexión consume ancho de banda, incluido el tráfico redundante. No se utilizan mecanismos de aseguramiento de la conexión para ciertos tipos de tráfico TCP/IP, con el fin de minimizar los paquetes con información no útil, cuando sea tolerable. La discriminación en el manejo de paquetes se logra seleccionando el protocolo de transporte:

- ▼ **TCP** Es el mecanismo orientado a la conexión para transportar paquetes IP a través de una interconexión.
- ▲ **UDP** Es el mecanismo sin conexión para el transporte de paquetes.

La principal diferencia entre los dos es que TCP requiere un mensaje ACK del receptor que reconoce la terminación exitosa de cada paso de una transmisión, mientras que UDP no. Ésta es la razón por la que suele conocérsele a UDP como el transporte sin conexión. Debido a que UDP no está orientado a la conexión, es más rápido y eficiente que TCP. UDP se utiliza para aplicaciones de red, donde se puede tolerar la retransmisión si un mensaje falla.

Tanto TCP como UDP operan en la capa 4 de la pila OSI, justo arriba de la capa de red IP. Las interconexiones envían tráfico TCP y UDP simultáneamente, pero es posible enviar un mensaje individual utilizando sólo uno de los dos. La diferencia entre los dos se manifiesta en el formato de envoltura de transporte del datagrama IP, llamada *segmento*. Cuando un flujo de paquetes se envía por una red IP, los paquetes se envuelven en un segmento TCP o uno UDP y se procesan de acuerdo con las reglas de ese protocolo de transporte en particular. Estos segmentos contienen los datos que se utilizan para transportar el paquete a través de la interconexión. Tenga en cuenta que no se trata de datos útiles, sino de información utilizada para administrar el transporte de los paquetes.

Un paquete que se envía por medio de una conexión TCP tiene un encabezado mucho más grande que uno que viaja por medio de UDP. Los campos extra en el encabezado TCP contienen información que se utiliza para establecer conexiones y manejar errores. TCP es el subsistema responsable de establecer y administrar las conexiones IP y utiliza un sofisticado mecanismo de identificación para asegurarse de que las dos estaciones terminales estén configuradas adecuadamente para transmitir. Por ejemplo, cuando hace clic en un hipervínculo para saltar a una nueva página Web, TCP entra en acción para identificarse con ese servidor Web, para que la página se descargue de manera apropiada. TCP también cuenta con procedimientos para la supervisión de transmisiones y la recuperación de errores.

El formato del segmento TCP

Los datagramas IP están colocados dentro de los segmentos TCP cuando el protocolo TCP administra el transporte. El formato del segmento TCP, que se muestra en la figura 2-14, contiene ciertas partes de datos para el establecimiento de conexiones TCP y la administración del transporte de paquetes.

Los campos de datos en el segmento TCP reflejan el enfoque del protocolo en el establecimiento y la administración de las conexiones de red. Cada uno de estos campos se utiliza para realizar una función específica que contribuye a asegurar que la conexión funcione sin problemas:

- **Puerto de origen** El puerto de aplicación utilizado por el host emisor.
- **Puerto de destino** El puerto de aplicación utilizado por el host receptor.
- **Número de secuencia** Coloca los datos del paquete para que quepa dentro del flujo general de paquete.
- **Número de reconocimiento** Contiene el número de secuencia del siguiente paquete TCP que se espera, reconociendo así implícitamente la recepción del mensaje anterior.

Número de bits	16	16	32	32	4	6	6	16
	Puerto de origen	Puerto de destino	Número de secuencia	Número de reconocimiento (ACK)	HLEN	Reservado	Bits de código SYN, FIN	Ventana

Figura 2-14. El segmento del paquete TCP contiene los datos que se utilizan para administrar de cerca el transporte del paquete.

- **HLEN** Indica la *longitud del encabezado* y le indica al receptor el tamaño que tendrá el encabezado, para que la CPU sepa dónde empieza el campo de datos.
- **Reservado** Son los bits reservados por la Internet Engineering Task Force (IETF) para uso futuro.
- **Bits de código** Contiene los bits SYN (de sincronización) que se utilizan para establecer una conexión o los bits FIN (de final) para terminarla.
- ▲ **Ventana** Contiene el número de bytes que la estación receptora puede almacenar o que habrá de enviarse. Este campo establece una "ventana de capacidad" para asegurarse de que el emisor no sature al receptor enviando muchos paquetes a la vez.

Establecimiento de una conexión de TCP

El proceso de conexión de TCP suele considerarse como un "saludo de tres vías", porque el segundo paso incluye el envío, por parte de la estación receptora de dos segmentos TCP al mismo tiempo. Los pasos de la figura 2-15 muestran un par de campos del segmento TCP en acción. El primer número de secuencia del segmento TCP sirve como número de secuencia inicial (el número base que se utiliza para mantener los paquetes subsecuentes en la secuencia adecuada). El campo Secuencia se utiliza para el reensamblado de los paquetes que se encuentran fuera de secuencia en un mensaje coherente en el extremo receptor.

En el ejemplo de la figura 2-15 se muestra una PC conectada a un servidor Web. Sin embargo, es posible conectar cualquier tipo de estación terminal: un servidor conectado a otro servidor para realizar una transacción de comercio electrónico, dos PC conectadas para llevar a cabo una sesión IRC (conectividad inter-regional) o cualquier otra conexión entre dos estaciones terminales en una red IP.

Ventaneo TCP

No basta con establecer la conexión; la sesión debe administrarse dinámicamente para asegurarse de que las cosas trabajen de manera correcta. La tarea principal consiste en asegurarse que una estación no sature a la otra transmitiendo demasiados datos al mismo tiempo.

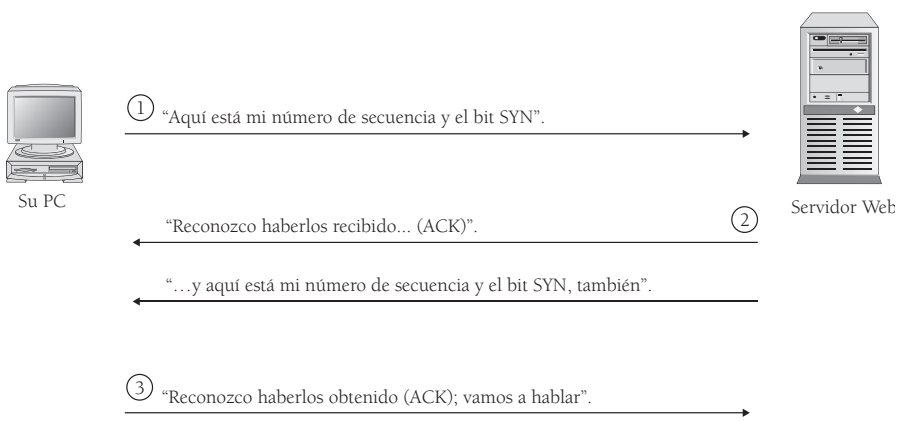


Figura 2-15. El proceso de saludo TCP de tres vías transfiere las señales SYN y ACK.

Esto se lleva a cabo por medio de una técnica llamada *ventaneo*, en que la estación receptora indica a la otra cuántos bytes está dispuesta a recibir. Visto de otra forma, la estación está diciendo la cantidad de memoria que tiene disponible para procesar los paquetes recibidos. El proceso de ventaneo de TCP se muestra en la figura 2-16, en que se observa a la izquierda un tamaño de ventana muy pequeño y uno adecuado a la derecha.

El tamaño de la ventana se comunica por medio de mensajes ACK. Obviamente, al observar la figura 2-16, un tamaño de ventana de 1 000 bytes no es suficiente porque provoca que se presente una relación uno a uno entre los paquetes entrantes y los ACK salientes (lo que representa demasiada información excedente en relación con el tráfico útil). En la mitad derecha de la figura 2-17 se muestra un mejor tamaño de ventana de 10 000 bytes. Como se muestra en la ilustración, esto permite que la estación emisora envíe todos los paquetes que desee, siempre y cuando el total acumulado permanezca por debajo del tamaño límite de la ventana de 10 000 bytes. Esto permite una relación más favorable entre la información útil y la excedente.

El mensaje en el área inferior derecha está sombreado para resaltar el hecho de que los tamaños de ventana se ajustan dinámicamente durante una sesión. Esto se hace debido a los cambios en las condiciones dentro de la estación receptora. Por ejemplo, si un servidor

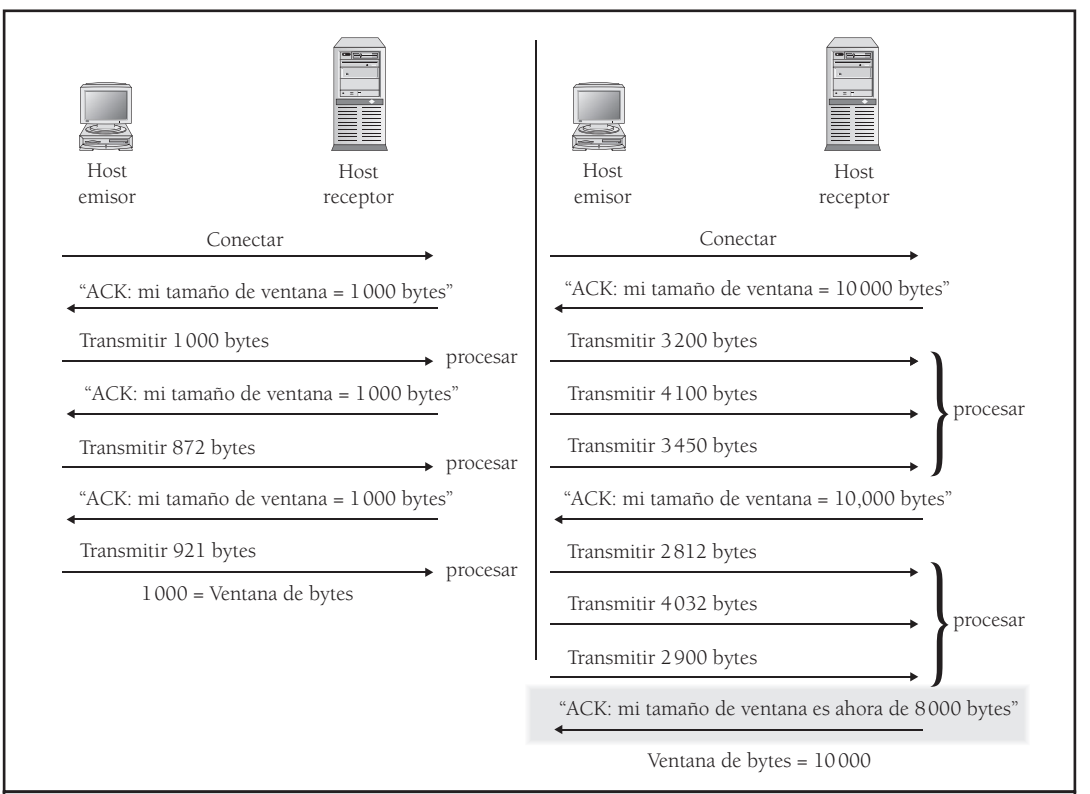


Figura 2-16. El ventaneo asegura que el host receptor tiene la capacidad de procesar paquetes entrantes.

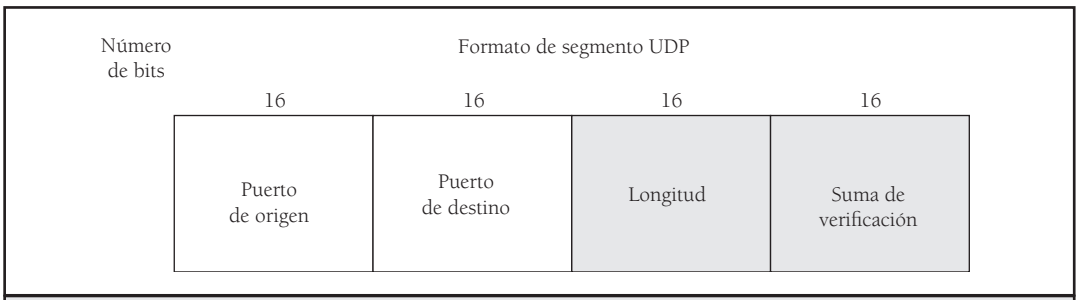


Figura 2-17. El formato del segmento UDP no tiene los campos Secuencia y Reconocimiento.

Web de pronto detecta conexiones provenientes de otros hosts emisores, éste dispondrá de una cantidad menor de memoria para procesar sus paquetes, y reducirá el tamaño de su ventana.

Manejo de paquetes IP no orientados a la conexión mediante UDP

El protocolo de datagrama de usuario (UDP) es sin conexión en el sentido de que no utiliza reconocimientos ni ventaneo. Comparado con TCP, UDP es un protocolo de transporte "del mejor esfuerzo" (simplemente transmite el mensaje y espera lo mejor). El formato del segmento UDP se muestra en la figura 2-17. Además de los números de puerto para indicar cuáles aplicaciones de red ejecutar, los segmentos UDP sólo declaran el tamaño de los paquetes. El único mecanismo de confiabilidad con el que cuenta UDP es la suma de verificación, que se utiliza para comprobar la integridad de los datos durante la transmisión. La probabilidad de que la suma de verificación de un paquete recibido que contenga datos alterados coincida con la suma del mensaje enviado es minúscula.

DIRECCIONAMIENTO IP

Para ir a cualquier lugar en Internet, debe teclear un localizador uniforme de recursos (URL) en el campo Dirección en su navegador. Un nombre único de dominio se combina con una categoría de organización, para formar un URL, como www.velte.com. En realidad, casi nunca es necesario teclear un URL; basta con hacer clic en un hipervínculo que tenga el URL almacenada en el HTML que integra la página Web que está dejando.

Los URL solamente existen para facilitar la navegación por Internet; no son direcciones IP reales. En otras palabras, si teclea el URL **www.velte.com** en su navegador, se envía una solicitud a un servidor DNS (configurado como servidor DNS principal en la configuración de red de las PC) para que traduzca el URL a IP, como se muestra en la figura 2-18.

Es necesaria la traducción a direcciones IP, porque los enrutadores y conmutadores que operan en Internet no reconocen los nombres de dominio. Por cierto, debe utilizarse una dirección IP sólo para que su solicitud llegue hasta el servidor DNS.

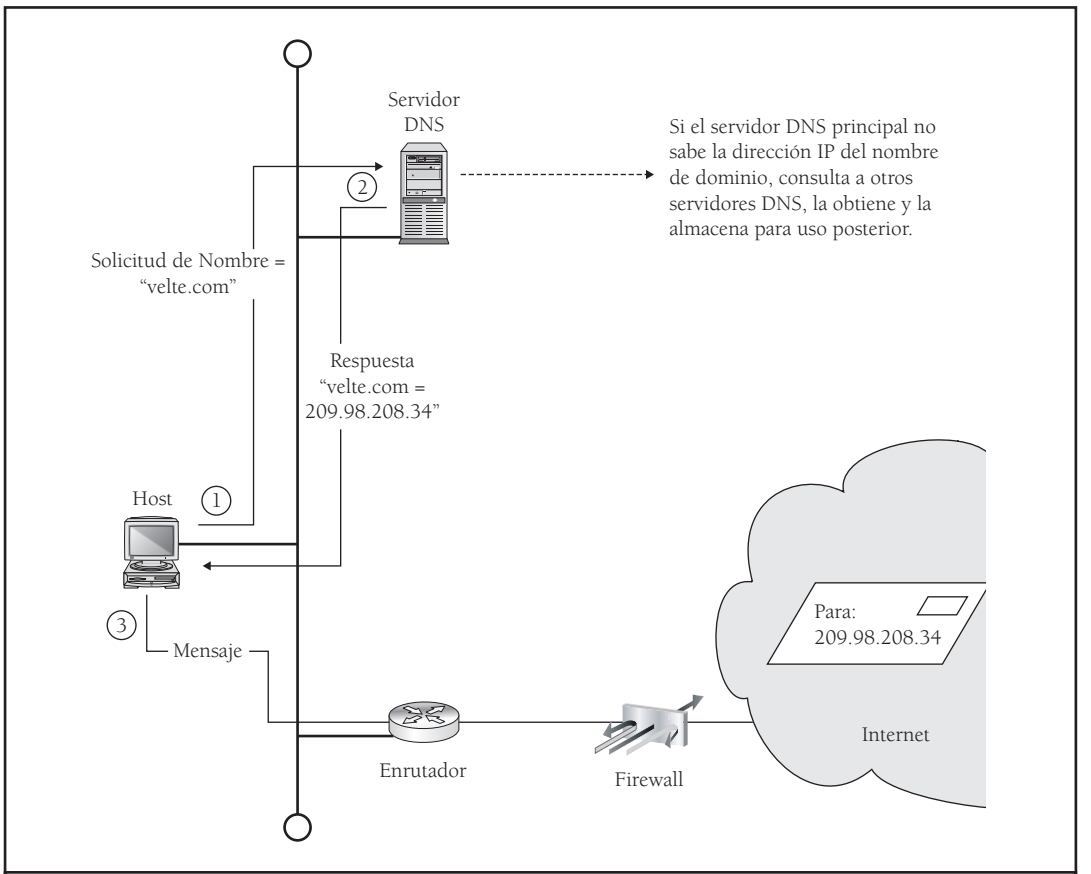


Figura 2-18. Los servidores DNS buscan las direcciones IP numéricas asignadas a los nombres de dominio.

Todas las direcciones en Internet son IP. La Internet Assigned Numbers Authority (IANA) asigna las direcciones IP. Los nombres de dominio solían ser otorgados por una organización llamada InterNIC (Internet Information Center). La principal responsabilidad de estas organizaciones fue asegurarse de que todas las direcciones IP y los nombres de dominio fueran únicos. Por ejemplo, www.velte.com fue otorgado por InterNIC; y su dirección IP en ese entonces, 209.98.208.34, fue otorgada por el ISP, que, por su parte, obtuvo la dirección IP de la IANA. La Internet Corporation for Assigned Names and Numbers (ICANN) empezó a funcionar a principios de 1999 para hacerse cargo de las tareas de asignación. En la actualidad, los ISP todavía asignan a los usuarios las direcciones IP. Sin embargo, los ISP obtienen sus direcciones IP de una oficina regional o nacional de registro de Internet (NIR).

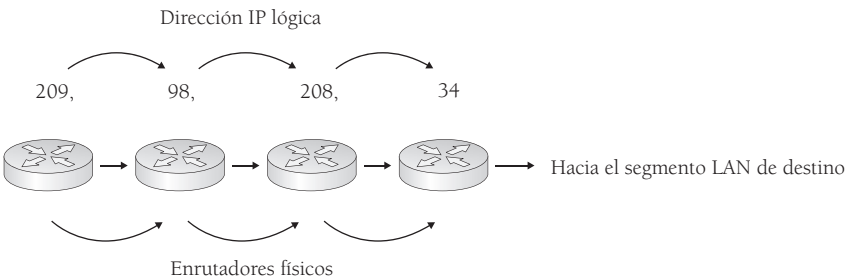
El formato de las direcciones IP

Cada nodo en Internet debe tener una dirección IP. Esto incluye a los hosts y a las redes. No hay forma de escapar a esta regla porque el direccionamiento IP es lo que mantiene unida

a Internet. Aún las estaciones conectadas a una LAN con su propio sistema de direccionamiento (como AppleTalk), deben traducirse a IP para ingresar a Internet.

Resulta irónico que, a pesar de la imposición de que toda dirección IP sea única en el mundo, al mismo tiempo todas las direcciones IP deben estar en el mismo formato. Las direcciones IP tienen una longitud de 32 bits y están divididas en cuatro secciones, cada una de 8 bits, llamadas *octetos*.

Los enrutadores utilizan direcciones IP para reenviar paquetes a través de interconexiones. Poniendo esto en términos más sencillos, a medida que el paquete salta de un enrutador a otro, avanza por varias redes hasta que llega al enrutador que tiene asignada la misma dirección que dicho paquete.



Desde luego, a veces un mensaje recorrerá varios enrutadores antes de acercarse a su destino. A veces es necesario dar varios saltos para encontrar el próximo destino.

De los bits al formato con punto decimal

Como ya se mencionó, las computadoras sólo comprenden las instrucciones y los datos en formato binario. Esto también es válido para las direcciones IP, pero se inventó el formato con punto decimal para que la gente pudiera leer las direcciones IP binarias. El *punto decimal* toma su nombre del hecho de que convierte los bits en números decimales por cada octeto, separados por puntos. En la figura 2-19 se muestra la conversión de una dirección IP al formato con punto decimal.

En la figura 2-19 también se muestran las dos direcciones reservadas. Suponiendo que una máscara de subred es de 24 bits, todos los unos del octeto son para transmisión, donde el enrutador automáticamente reenvía un mensaje a todos los hosts conectados a las redes direccionadas hasta ese punto de la dirección. Por ejemplo, los mensajes dirigidos a 220.151.102.255 se enviarán a todas las interfaces cuyos primeros tres octetos sean 220.151.102. La otra dirección reservada (llamada la dirección de "esta red") se usa para fines técnicos que no se analizarán aquí. Basta con que comprenda que una dirección como 220.151.102.0 significa "esta interfaz" en la red 220.151.102. Un aspecto que hay que tomar en cuenta es que la máscara de subred y sólo la máscara de subred definen lo que son las ID de red y la transmisión. Por ejemplo, 10.255.0.10 con una máscara de subred 255.255.255.0 es una dirección IP válida, a pesar de que el segundo octeto está formado solamente por unos y el tercero solamente por ceros. De manera similar, 10.1.1.0, con una máscara de subred 255.255.240.0 y sólo unos en el cuarto octeto *no* es la dirección de transmisión, ni un cuarto octeto con sólo ceros sería la red. Puesto que la máscara es de 20 bits, *todos* los 12 bits finales deben ser unos para transmisión o ceros para indicar la red.

Primer octeto en binario

128	64	32	16	8	4	2	1
1	1	0	1	1	1	0	0

128 + 64 + 0 + 16 + 8 + 4 + 0 + 0 = 220

Segundo octeto en binario

128	64	32	16	8	4	2	1
1	0	0	1	0	1	1	1

128 + 0 + 0 + 16 + 0 + 4 + 2 + 1 = 151

Tercer octeto en binario

128	64	32	16	8	4	2	1
0	1	1	0	0	1	1	0

0 + 64 + 32 + 0 + 0 + 4 + 2 + 0 = 102

Cuarto octeto en binario

128	64	32	16	8	4	2	1
0	0	0	1	1	0	0	1

0 + 0 + 0 + 16 + 8 + 0 + 0 + 1 = 25

Octeto para transmisión

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Octeto para red

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	= 0

Figura 2-19. Las direcciones IP que usted observa en el formato con punto decimal están definidas por treinta y dos bits.

Clases de direcciones IP

La Internet Engineering Task Force (IETF) divide a las direcciones IP en tres clases generales (más dos especializadas). Como se mencionó, las direcciones IP se dividen en cuatro octetos con punto decimal. En la figura 2-20 se muestran los primeros rangos de los octetos. Los octetos sombreados muestran cuánta cantidad de espacio de las direcciones IP está reservado para el direccionamiento de redes. A medida que la porción sombreada se mueve hacia la derecha, hay más redes posibles, pero menos hosts.

A esta designación de rangos se le denomina la *regla del primer octeto*. Cualquier enrutador en el mundo puede leer el primer octeto de una dirección IP y saber cuáles bits interpretar como parte de la dirección de la red en comparación con la dirección de host. Si los enrutadores no pudieran hacer esta distinción, Internet no funcionaría.

Casi todas las redes se numeran utilizando direcciones IP Clase B o Clase C. El primer octeto varía en cada clase de la manera siguiente:

		Octeto 1		Octeto 2		Octeto 3		Octeto 4
Clase A	Primer rango de octetos 1-126	Red	.	Host	.	Host	.	Host
	Ejemplo:	52.		0.		0.		0.
Clase B	Primer rango de octetos 128-191	Red	.	Red	.	Host	.	Host
	Ejemplo:	178.		123.		0.		0.
Clase C	Primer rango de octetos 192-223	Red	.	Red	.	Red	.	Host
	Ejemplo:	220.		78.		201.		0.

Figura 2-20. Las tres clases de dirección IP difieren por los octetos que utilizan para sus direcciones de red.

- ▼ **De 0 a 127** Clase A, el rango de los números de red es de 0.0.0.0 a 127.0.0.0 para 128 redes. Sin embargo, la red no debe consistir de ceros solamente y 127.0.0.0 está reservada para hacer un ciclo hacia atrás. Lo que queda son 126 redes (de 1 a 126). Existen 16 777 214 posibles direcciones de host (16 777 216 menos 2).
- ■ **De 128 a 191** Clase B, el rango de los números de red es de 128.0.0.0 a 191.255.0.0 para 16 384 redes. Existen 65 534 posibles direcciones de host (65 536 menos 2).
- ▲ **De 192 a 223** Clase C, el rango de los números de red es de 192.0.0.0 a 223.255.255.0 para 2 097 152 redes. Existen 254 posibles direcciones de host (256 menos 2).

A medida que analice la lista anterior, se podrá imaginar que sólo algunas organizaciones y provedores de servicios muy grandes tienen direcciones clase A (en realidad, sólo 126 de ellos).

NOTA No olvide que una red, de acuerdo con la definición estricta, es un segmento LAN (un medio de acceso individual compartido). Esto es lo que significa la palabra "red" en el contexto del direccionamiento IP. Una red (o segmento LAN) también está identificado como una interfaz de red (o interfaz, para abreviar), porque sólo es posible conectar una red a una interfaz del enrutador. Por ejemplo, tal vez los empleados consideren a la intranet de Ford Motor Company como una red, pero el administrador de la red de Ford debe

asignar direcciones IP únicas a las decenas de miles de redes individuales (segmentos LAN) conectadas a las interfaces de los enrutadores de la compañía.

Direccionamiento privado

La IANA reservó tres bloques de direcciones IP para direcciones privadas. Una de éstas es una dirección que no está registrada en la IANA y no se utilizará más allá de las fronteras de la interconexión empresarial (en otras palabras, no en Internet). A las interconexiones numeradas de forma privada también se les conoce como *internets privadas*, pero en este libro las llamamos "interconexiones" para evitar confusiones. Los tres bloques de espacio para las direcciones privadas reservadas son las siguientes:

- ▼ **10.0.0.0 a 10.255.255.255** El *bloque 10* es un solo número de red clase A.
- ■ **172.16.0.0 a 172.31.255.255** El *bloque 172* consta de 16 números contiguos de red clase B.
- ▲ **192.168.0.0 a 192.168.255.255** El *bloque 192* consta de 256 números contiguos de red clase C.

Es necesario asignar direcciones IP públicas a los *dispositivos de extremo*, como los firewalls y los enrutadores de frontera, para hacer negocios con el mundo exterior. Las direcciones privadas se asignan sólo a hosts que hacen todas o casi todas sus conexiones dentro de la interconexión privada.

Sin embargo, eso no quiere decir que un host direccionado de manera privada no pueda conectarse con el mundo exterior. Se utilizan dos servicios de traducción de direcciones IP para asignar temporalmente números IP de Internet públicos válidos a hosts con direcciones IP privadas permanentes. Una técnica es la traducción de direcciones de red (NAT) y la otra la traducción de direcciones de puertos (PAT).

La NAT es una correlación uno a uno, mientras que la PAT es una traducción uno a varios. Es decir, NAT asigna una dirección IP única a cada host cuando se conecta a Internet. Es muy probable que esta dirección cambie cada vez que el host se vuelva a conectar. Por otra parte, PAT asigna los hosts a una dirección IP única utilizando puertos diferentes.

En la figura 2-21 se muestra cómo trabajan las dos.

Por lo general, un firewall realiza la traducción de direcciones. Tenga presente que estas traducciones de privadas a públicas son temporales. Con NAT, cuando el host interno termina su conexión hacia el mundo exterior, la dirección IP pública vuelve al grupo de direcciones para su reutilización.

La ventaja evidente del direccionamiento privado es que se tiene espacio para direcciones casi ilimitado con el fin de numerar redes y hosts internos. Con un firewall o un enrutador de orilla adecuadamente configurado para efectuar la traducción de direcciones NAT y PAT, estos hosts con direcciones privadas aún tienen la posibilidad de conectarse a Internet. Más aún, debido a que sus direcciones reales son "traducidas" por un número asignado temporalmente, los hackers no pueden encontrar ningún indicio de la topología de la interconexión privada.

Subredes

La creación de *subredes* es la práctica de obtener más direcciones de red a partir de una determinada dirección IP, que estén disponibles en forma predeterminada. Como se mencionó,

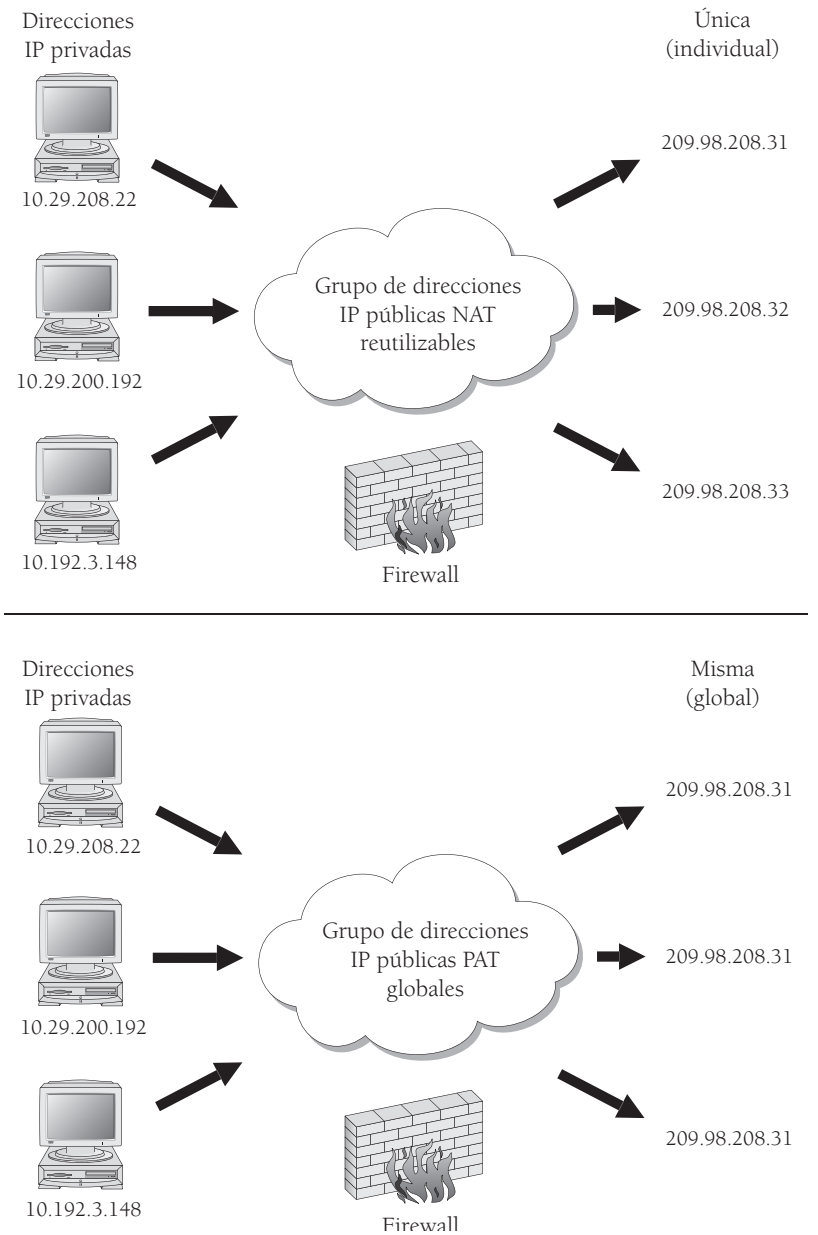
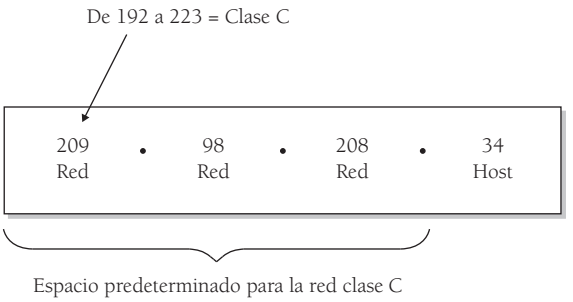


Figura 2-21. NAT asigna temporalmente direcciones públicas, reutilizables; PAT asigna una dirección IP global.

las clases de dirección IP definen cuáles bits proporcionan direcciones, en forma predeterminada, a las redes en comparación con los hosts. El significado de *predeterminado* aquí, es que una vez que se haya leído el primer octeto de una dirección, el enrutador sabe a cuáles bits debe tratar como bits de direcciones de red. Tomando una dirección clase C como ejemplo, el enrutador verá en forma predeterminada los primeros tres octetos como bits de red y el octeto final como bits de host.



Sin embargo, en la realidad, casi todas las empresas necesitan más espacio para direcciones de red que el que les asignan sus ISP. Lo anterior genera la necesidad de "hacer trampa" al reclamar algunos de los bits de host en forma predeterminada para utilizarlos en el direccionamiento de redes. Esto se realiza al reasignar bits de la porción del host de la dirección IP a la porción de red. En la figura 2-22 se muestran dos direcciones IP, una clase B de subred y la otra clase C. Ambas se muestran en formato con punto decimal y en formato binario.

Es importante saber a qué clase pertenece la dirección IP, porque las subredes se extienden hacia la derecha, comenzando en el bit que se encuentra en el extremo izquierdo del espacio predeterminado de direcciones de red. En otras palabras, sólo las posiciones de bit que se encuentran en las porciones sombreadas de la figura 2-22 pueden ser invadidas por las direcciones de subred.

Tome en cuenta que casi todas las empresas tienen asignadas direcciones clase C, lo que significa que sólo cuentan, como máximo, con ocho bits para trabajar. En realidad, a muchas redes sólo se les asigna un rango de números de hosts, como 221.198.20.32-47.

Ejemplo de una subred formada de octetos completos

Las subredes hacen un uso más eficiente de las direcciones IP sin necesidad de modificarlas. Considere la red de la figura 2-23 como ejemplo. A la empresa se le asignó la dirección IP pública clase B 151.22.0.0 y se hizo funcionar como subred el tercer octeto completo.

Si observa la configuración de la figura 2-23, verá que existe espacio de direccionamiento para 254 subredes, con un espacio para 254 hosts por subred. El host sombreado en el área de la parte inferior derecha muestra una dirección de subred completa (en este ejemplo, el host número 1 conectado a la subred número 2 dentro de la dirección IP 151.22.0.1). Lo importante de este ejemplo es que el octeto completo (el tercero) está en una subred.

A medida que los enrutadores remotos se abren camino a través de las direcciones que están en subred de la figura 2-23, los paquetes automáticamente caerán en la interfaz correcta en el enrutador de extremo que se encuentra en la parte central inferior de la nube.

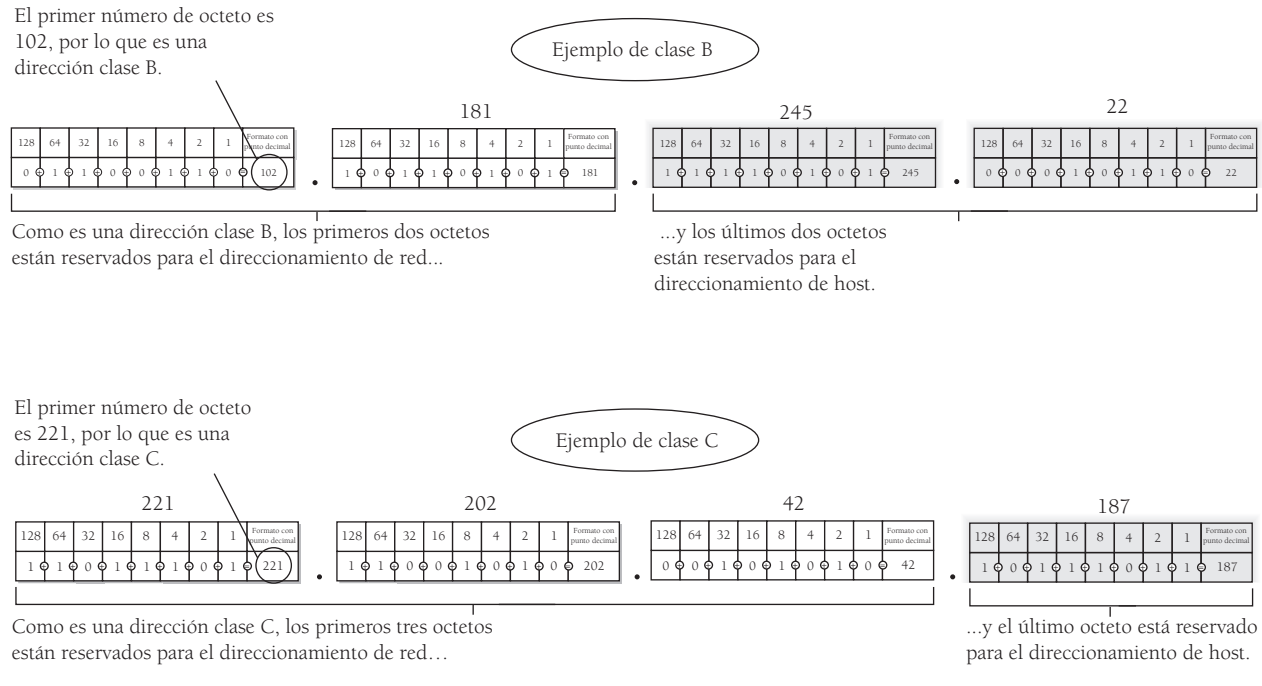


Figura 2-22. La creación de subredes amplía hacia la derecha el espacio asignado a las direcciones de red.

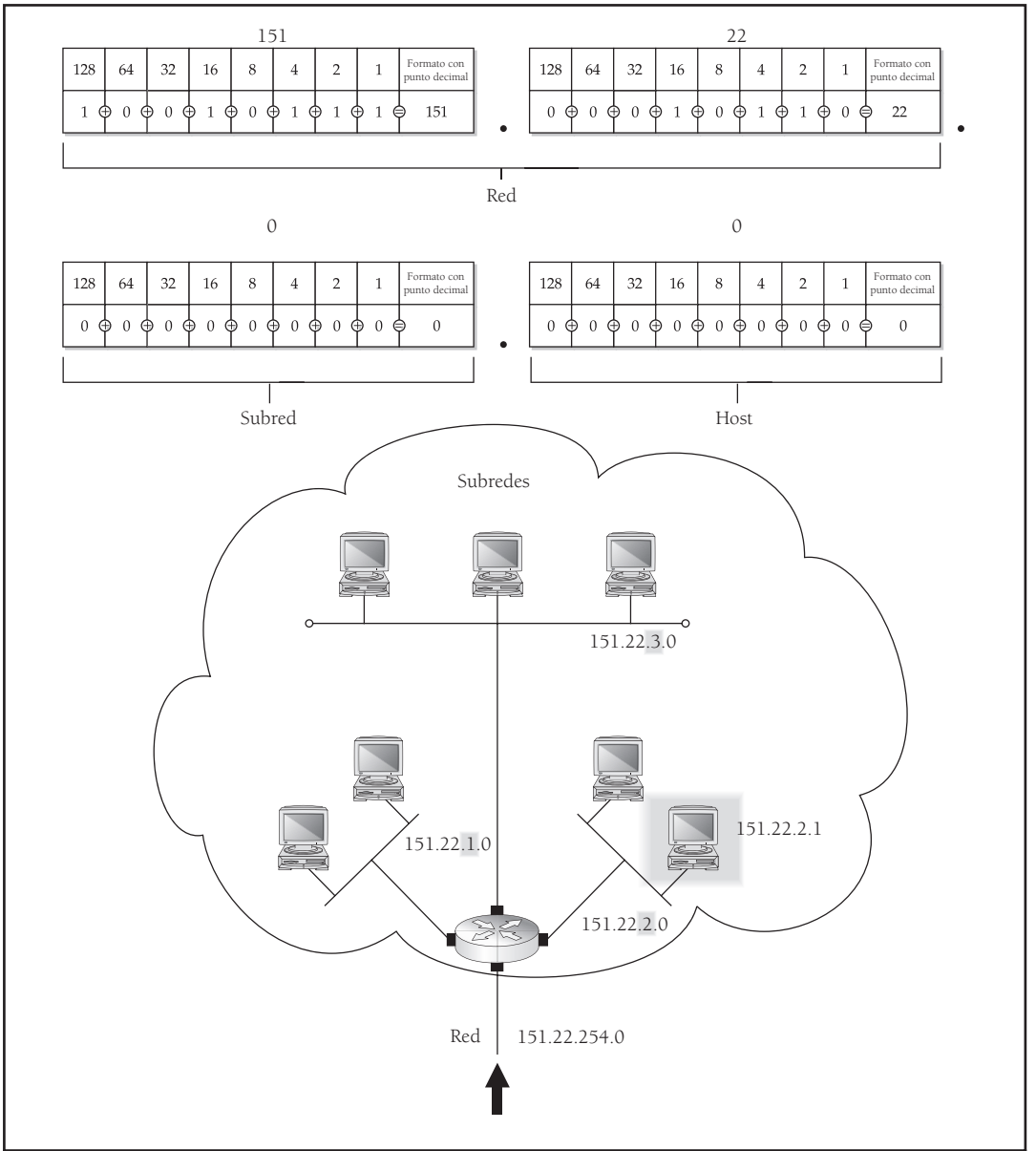


Figura 2-23. La creación de subredes hace eficiente el uso de espacio de direcciones; este ejemplo de clase B tiene espacio para 254 subredes.

La apariencia de las máscaras de subred y dónde se encuentran

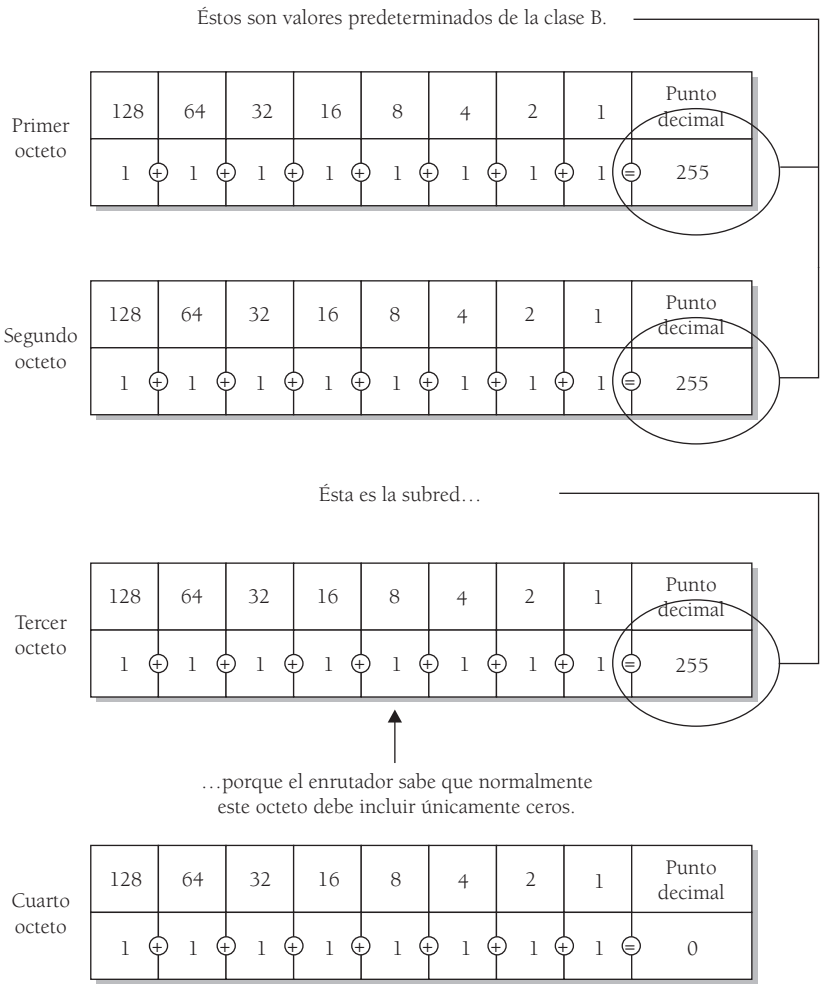
Todas las máscaras de subred tienen una longitud de 32 bits. Tome en cuenta que las máscaras no son direcciones; son plantillas que definen la manera como se utilizará una dirección IP. Difieren de las direcciones IP de dos maneras importantes:

- **Forma** Una máscara de subred está representada como una cadena de unos en binario o un número (como 255, en formato con punto decimal).
- **Ubicación** Se aplica una máscara de subred a una interfaz de red de un host específico y dentro del archivo de configuración del enrutador al que esté conectada la subred.

El archivo de configuración es administrado por el software IOS del enrutador Cisco. Un segmento LAN conectado se convierte en una subred al ingresar una instrucción como ésta:

```
MiEnrutador(config-if)#ip address 151.22.1.1 255.255.255.0
```

El comando MiEnrutador(config-if)# significa, "Configura esta interfaz de red en este enrutador", donde el comando se está ingresando a un enrutador Cisco llamado MiEnrutador. El comando **ip address** se utiliza para configurar la dirección IP de la interfaz de red. La dirección IP adecuada de la interfaz es 151.22.1.1 (dirección clase B) y los octetos subsecuentes 255.255.255.0 instruyen al enrutador para que todo el tercer octeto funcione como red, representado en bits como:



Esto no es demasiado complicado. Una máscara de subred es una cadena de unos contiguos que se extiende desde el extremo del espacio de dirección de red en la parte del host. La ubicación de ese punto depende de la clase de dirección (el ejemplo anterior es una clase B). La máscara de subred se ingresa en el archivo de configuración del enrutador utilizando el comando **ip address** para agregar la máscara de subred a la dirección IP normal y aplicarla a una interfaz específica de red (y, por lo tanto, a un segmento LAN específico).

Creación de subredes por octeto parcial

Sin embargo, las subredes casi nunca son tan simples. Esto se debe a que la mayor parte de las empresas tienen asignadas direcciones IP clase C, donde sólo está reservado el cuarto octeto, en forma predeterminada, para espacio de direcciones de host. En estos casos, la máscara de subred se extiende de manera parcial en el espacio de direcciones de host y, por lo tanto, se representa con un número con punto decimal menor a 255.

La parte sombreada de la figura 2-24 representa los bits de host reservados para la subred del cuarto octeto. Observe que sólo se solicitó la mitad de los bits y no los ocho. Esta es una de las llamadas máscaras .240 (que permite hasta 14 subredes). Cada subred de este ejemplo cuenta con espacio suficiente de direcciones para 14 hosts (para un total de 196 posibles hosts). Este ejemplo se ingresa en el archivo de configuración del enrutador de la manera siguiente:

```
MiEnrutador(config-if)#ip address 209.98.208.34 255.255.255.240
```

Este comando le indica al enrutador que la interfaz está conectada a una subred con 28 bits de ID de red y 4 bits de ID de hosts. A partir de aquí, la entrega de paquetes en la subred es automática.

Es posible elegir entre varias máscaras de subred, como se muestra en los ejemplos de direcciones clase C de la tabla 2-1. Cuanto más a la derecha se extienda una máscara hacia el espacio de direcciones de host, menor será el número posible de hosts por subred. La máscara que se utilizará depende totalmente de las necesidades de la organización. Por ejemplo, si una interfaz de red en un enrutador está conectada a un vínculo punto a punto hacia una oficina remota, sólo se requieren dos direcciones de host (una en cada extremo). En este escenario, tendría sentido utilizar la máscara .252, que sólo tiene dos direcciones de host.

Máscara de subred	Bits de ID de red	Bits de ID host	Notación de ejemplo	Número de subredes	Número de hosts por subred
.192	26	6	209.98.208.34/26	2	62
.224	27	5	209.98.208.34/27	6	30
.240	28	4	209.98.208.34/28	14	14
.248	29	3	209.98.208.34/29	30	6
.252	30	2	209.98.208.34/30	62	2

Tabla 2-1. Lista de máscaras de subred ordenadas por número de bits de ID de red.

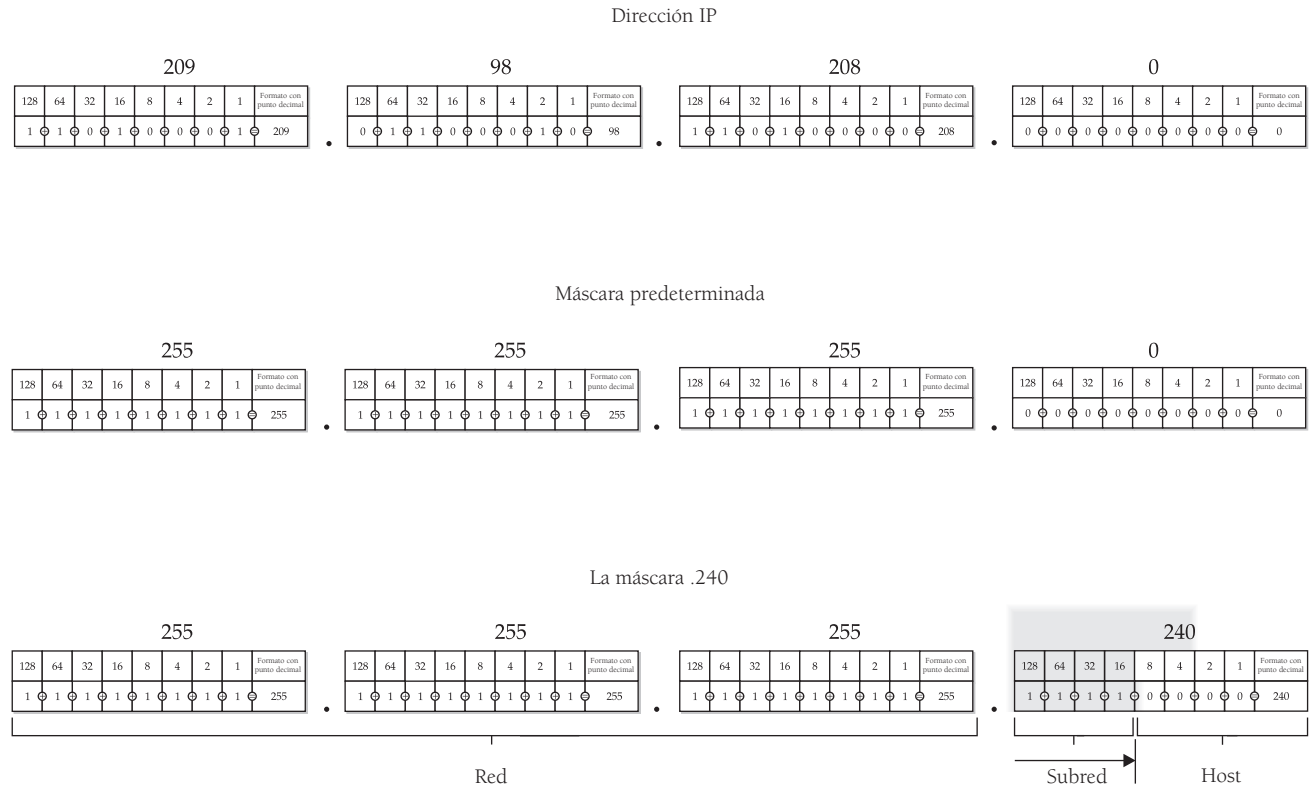


Figura 2-24. Por lo general, sólo una parte de un octeto es de subred, como en el ejemplo clase C.

Versión 6 de IP

Aunque el sistema de direccionamiento de Internet parezca trabajar correctamente y sin problemas, la verdad es que las direcciones IP se están acabando. En realidad. Al parecer, IPv4, el sistema de direccionamiento de 32 bits que se utiliza en la actualidad, ofrece un número de direcciones más que suficiente. De hecho, con IPv4 existen casi cuatro mil millones de direcciones disponibles. Sin embargo, necesitamos más.

Cuando se desarrolló el esquema de direccionamiento IP en la década de 1980, nadie tenía en mente que Internet se convertiría en el gigante descomunal que es ahora. El enorme crecimiento de Internet está devorando direcciones IP (no sólo computadoras, servidores y otros equipos de red utilizan direcciones IP, sino que a medida que otros dispositivos, como teléfonos celulares y PDA con servicios de Internet están ganando popularidad, será necesario un mayor uso de direcciones IP).

Entra en escena IPv6, también conocido como IPng ("ng" significa "nueva generación").

IPv4 utiliza un número binario de 32 bits para identificar redes y estaciones terminales únicas. Esto permite que se puedan tener alrededor de cuatro mil millones de direcciones diferentes. IPv6 es distinto, porque utiliza un formato hexadecimal de 128 bits (los números van de 0000 a FFFF). Este esquema de direccionamiento permite un número de hosts únicos igual a 10^15, o 340 282 366 920 938 463 463 374 607 431 768 211 456 direcciones totales. En esencia, eso representa una sola dirección por cada grano de arena en el planeta.

Aparte del crecimiento exponencial de direcciones IP, IPv6 tiene mejoras funcionales en relación con IPv4, entre las que se incluyen:

- ▼ Formato simplificado del encabezado.
- ■ Eficiencia mejorada de enrutamiento, al utilizar una arquitectura jerárquica de red.
- ■ Soporte a protocolos de enrutamientos muy conocidos.
- ■ Configuración automática.
- ■ IPSec incrustado.
- ▲ Mayor número de direcciones de transmisión múltiple.

Formato

Como ya se indicó, las direcciones IPv6 tienen un tamaño de 128 bits. Se expresan como ocho campos de 16 bits, con números en notación hexadecimal (de 0000 a FFFF), en este formato:

```
x:x:x:x:x:x:x:x
```

Como ejemplos de este formato se tiene:

```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
```

o

```
1080:0:0:0.8:800:200C:417A
```

Las direcciones IPv6 pueden representarse de tres maneras:

- ▼ El método más directo consiste simplemente en ingresar los valores en cada uno de los ocho campos, de la manera siguiente:

  ```
  1070:200:0:0:900:300C:618A
  ```

Notará que no es necesario utilizar los ceros al principio de un determinado campo (o sea, "200" es lo mismo que "0200").

- En algunos casos, las direcciones IPv6 contendrán largas cadenas de ceros. Como tal, los diseñadores del esquema de direccionamiento IPv6 han ideado una manera de no utilizar la tecla "0" del teclado. En lugar de teclear "0000:0000:0000:0000:0000:0000:1" o "0:0:0:0:0:0:0:1", es aceptable indicar dos o más grupos de ceros utilizando "::.". De esta forma, el ejemplo mencionado anteriormente puede abreviarse como "::: 1".
  La única desventaja de esta forma abreviada es que la notación "::" sólo puede usarse una vez en la dirección. Con ella, IPv6 puede determinar que todos los valores "que faltan" deben ser ceros. Sin embargo, si la notación "::" se utiliza más de una vez, sería imposible saber cuántos grupos de ceros faltarían en cada sección.
  En la tabla 2-2 se muestra cómo pueden abreviarse las diferentes direcciones IPv6.
- Por último, dado que tendrá que pasar una buena cantidad de tiempo antes de que se adopte el IPv6 totalmente, existe un formato que se utiliza en ambientes que mezclan ambas versiones. Dicho formato combina ambos y se representa como:

  ```
  x:x:x:x:x:x:d.d.d.d
  ```

  En este caso, las "x" representan los valores hexadecimales de los seis grupos de 16 bits de orden elevado de la dirección y las "d" representan los valores decimales de los cuatro grupos de 8 bits de orden inferior. Por ejemplo:

  ```
  0:0:0:0:0:FFFF:129.144.40.20
  ```

  Para complicar un poco las cosas, aún puede utilizar la forma comprimida de las direcciones, incluso en el formato mezclado. Por ejemplo:

  ```
  ::FFF:129:144:40:20
  ```

Tipo de direcciones	Dirección IPv6	Representación utilizando ::
Una sola transmisión	1070:200:0:0:900:300C:618A	1070:200::900:300C:618A
Transmisiones múltiples	FF01:0:0:0:0:0:0:100	FF01::100
Ciclo de retorno	0:0:0:0:0:0:0:1	::1
Dirección no especificada	0:0:0:0:0:0:0:0	::

Tabla 2-2 Abreviatura de direcciones IPv6.

Prefijo IP

El prefijo IPv6 es la parte de la dirección que representa los bits de orden superior, del extremo izquierdo. Estos bits representan el identificador de red. El prefijo IPv6 se representa utilizando la notación de longitud prefijo/prefijo. Por ejemplo, 2001/16 identifica Internet, mientras que 2001:AB18/32 puede identificar a un ISP. Y la dirección 2001:4637:0:2930/64 identifica una red específica.

Tipos de direccionamiento

Existen tres tipos de direccionamiento disponibles en IPv6:

- **Una sola transmisión** Un host transmite a otro en una red. Cisco soporta cinco tipos de direcciones de una sola transmisión:
  - **Direcciones globales de una sola transmisión**, que son comparables a las direcciones de una sola transmisión globales IPv4. Es decir, se trata de una dirección IPv6 con el prefijo de una sola transmisión global. Las direcciones globales de una sola transmisión ascienden por las organizaciones y después a los ISP. Las direcciones globales de una sola transmisión contienen un prefijo de enrutamiento global, un ID de subred y una ID en la interfaz. Con excepción de las que comienzan con 000, todas las direcciones globales de una sola transmisión tienen una interfaz de 64 bits. En la actualidad, la asignación global de una sola transmisión utiliza un rango de direcciones que comienza con el valor 001 (2000::/3). Las direcciones globales de una sola transmisión utilizan un octavo del espacio de dirección de IPv6 total e integra el bloque más grande de direcciones asignadas.
    En la figura 2-25 se muestra el formato de direccionamiento de una sola transmisión global.
  - **Direcciones de una sola transmisión en sitio local**, que son similares a las direcciones privadas (como 10.0.0, 172.16.0.0 y 192.168.0.0) en IPv4.
  - **Direcciones locales de enlace de una sola transmisión,** que se utilizan para el descubrimiento del vecino y para configuración automática. Por ejemplo, estas direcciones se utilizan en una red cuando no está presente un enrutador.
  - **Direcciones IPv6 mapeadas en IPv4,** que se utilizan para representar las direcciones de un nodo IPv4 como una dirección IPv6.
  - **Direcciones IPv6 compatibles con IPv4,** que se utilizan de manera transitoria cuando IPv6 se emplea en redes IPv4 existentes.
- **Transmisiones a todas partes** Un host transmite al host de destino más cercano. La transmisión a todas partes se diseñó para que un host inicie la actualización de la tabla del enrutador de un grupo de hosts. IPv6 puede determinar cuál host de gateway está más cerca y envía paquetes a ese host, de manera única. A su vez, ese host puede transmitir a cualquier host del grupo, y así sucesivamente, hasta que todas las tablas de enrutamiento se hayan actualizado. Una dirección de transmisión a todas partes es una dirección global de una sola transmisión que se asigna a un grupo de interfaces que pertenecen a nodos diferentes.
- **Transmisión múltiple** Un host transmite a varios hosts en una red. El esquema de direccionamiento de transmisión múltiple utiliza direcciones con un prefijo

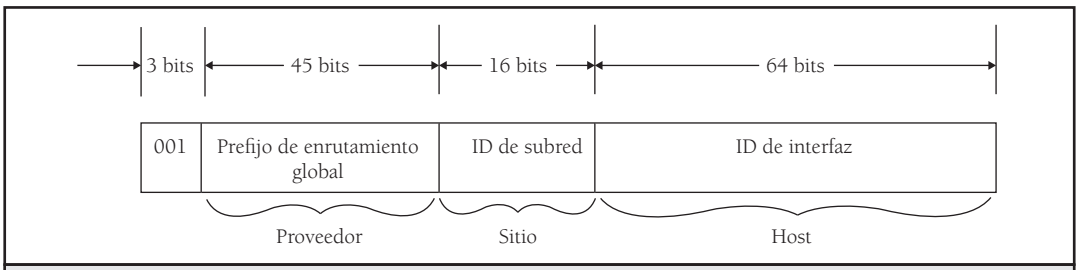


Figura 2-25. Formato de una dirección IPv6 global de una sola transmisión.

FF00::/8. En total, el rango de direcciones de transmisión múltiple utiliza 1/256 del espacio total de direcciones de IPv6. El segundo octeto después del prefijo establece el tiempo de vida y alcance de las direcciones de transmisión múltiple. Las que son permanentes tienen el parámetro de tiempo de vida en 0; las direcciones temporales están fijas a 1. Los 4 bits siguientes se utilizan para establecer el alcance de la dirección.

En la figura 2-26 no sólo se muestra la dirección de transmisión múltiple, sino también incluye los valores de estos bits. Para identificar las funciones específicas, cada bloque de direcciones de transmisión múltiple dentro del rango FF00:: a FF0F:: se utiliza para lo siguiente:

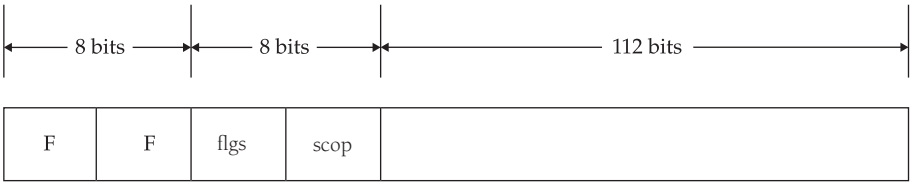
- **FF01::1** Todos los nodos dentro del alcance local de la interfaz.
- **FF02::1** Todos los nodos en el vínculo local.
- **FF01::2** Todos los enrutadores dentro de alcance local de la interfaz.
- **FF02::2** Todos los enrutadores en el alcance del vínculo local.
- **FF05::2** Todos los enrutadores en el sitio local.
- **FF02::1:FFXX:XXXX** Dirección de transmisión múltiple solicitada por el nodo (XX:XXXX representa los últimos 24 bits de la dirección IPv6 del nodo).

Configuración

Con IPv4, las direcciones se asignan de una de dos maneras:

▼ **Estáticamente** La dirección debe ingresarse manualmente.
▲ **Dinámicamente** DHCP/BOOTP asigna de manera automática direcciones IP a un host cuando ingresan en la red.

IPv6 utiliza un medio llamado *configuración automática sin estado*. Es similar a DHCP en que las direcciones IP se asignan de manera automática; sin embargo, difiere porque no se requiere una aplicación DHCP o un servidor especial. Con el uso del DHCP, cualquier enrutador que utilice una dirección IPv6 se convierte en un "proveedor" de direcciones IP de la red a la que esté conectado. Para evitar la duplicación de direcciones, IPv6 utiliza un medio llamado *detección de direcciones duplicadas (DAD).*



flgs: 0—Permanente
1—Transitorio

scop: 0—reservado
1—alcance de interfaz local
2—alcance de vínculo local
3—reservado
4—alcance administrado localmente
5—alcance local
6—(no asignado)
7—(no asignado)
8—alcance de organización local
9—(no asignado)
A—(no asignado)
B—(no asignado)
C—(no asignado)
D—(no asignado)
E—(no asignado)
F—(no asignado)

Figura 2-26. Las direcciones IPv6 de transmisión múltiple contienen información específica del tiempo de vida y el alcance de las direcciones.

Asignación de direcciones

Al igual que en IPv4, no puede elegir simplemente una dirección IP y tomarla para sí (aunque aparentemente exista una cantidad ilimitada de ellas). La IANA administra las direcciones IPv6 de manera muy parecida a las IPv4. Ha asignado el rango de direcciones 2001::/16 a registros del espacio de direcciones completo. Cada registro tiene un prefijo /23 dentro del espacio de direcciones 2001::/16. Las direcciones se asignan de la manera siguiente:

- ▼ **2001:0200::/23** y **2001:0C00::/23** Se utiliza en Asia. Estas direcciones se asignaron al Asia Pacific Network Information Centre (APNIC).
- ■ **2001:0400::/23** Se utiliza en América. Las direcciones fueron asignadas al American Registry for Internet Numbers (ARIN).
- ▲ **2001:0600::/23 y 2001:0800::/23** Se utilizan en Europa y el Medio Oriente. Estas direcciones se asignaron a Reseaux IP Européens, Network Coordination Center (RIPE NCC).

Después, los registros asignan el prefijo /32 a los ISP de IPv6 y, después, los ISP asignan un prefijo /48 a cada cliente. El prefijo /48 de cada sitio puede asignarse a cada LAN, utilizando un prefijo /64. Cada sitio puede tener un máximo de 65 535 LAN.

Direcciones IPv6 en un URL

Puesto que los dos puntos (:) ya se utilizan para identificar un número de puerto específico en un URL (por ejemplo, www.estoesunaprueba.com:8080), no puede usarse dentro de la dirección. Por lo tanto, es necesario encontrar una forma de utilizarla en navegadores Web. La forma que se escogió para que las direcciones IPv6 funcionen como URL es encerrarlas en corchetes, de la forma siguiente:

```
http://[2001:0401:3:4F23::AE35]
```

Si quisiéramos ir a un puerto específico utilizando una dirección IPv6, los dos puntos y el número de puerto irían a continuación de la dirección de la forma siguiente:

```
http://[2001:0401:3:4F23::AE35]:8080
```

Una vez dicho esto, utilizar IPv6 como URL es un problema enorme. Resulta mejor utilizar el nombre de dominio plenamente calificado que enredarse con la dirección IPv6. Después de todo, ¿no es más fácil recordar www.estoesunaprueba.com que 2001:0401:3:4F23::AE35?

IPv6 no va desplazar a IPv4 pronto. Existe una gran cantidad de expertos que piensan que a IPv4 no se le terminará el espacio para direcciones en más de una década y que IPv6 no representa en realidad nada nuevo o revolucionario para IP. Se esté de acuerdo con esto o no, es importante saberlo, porque muchos dispositivos de Cisco están listos para utilizar el sistema de direccionamiento IPv6. Sin embargo, a estas alturas, prácticamente toda la interconectividad se logra con el uso del protocolo de 32 bits y cuatro octetos, IPv4.

INTEGRACIÓN

¿Qué pasa tras bambalinas cuando se conecta a Internet? Tomemos el escenario más cotidiano, la descarga de una página Web.

Su PC envía paquetes UDP a su servidor DNS local para traducir el nombre de dominio a una dirección IP y regresa los resultados. Si se presenta un problema, terminará la búsqueda en DNS y el navegador enviará un mensaje diciendo que el servidor no se encontró.

La dirección IP de destino se inserta en el encabezado de sus paquetes, junto con su dirección IP y el número de puerto para HTTP (80). Su solicitud se envía mediante el transporte TCP al host de destino para establecer una conexión. La elección de la ruta que tome al destino se deja a los enrutadores, que leen la dirección IP y saltan de enrutador en enrutador para llegar a su destino. Si los paquetes no encuentran el host de destino, es muy probable que aparezca un mensaje de error que diga “destino inalcanzable”; o si existe un ciclo de enrutamiento, el contador Tiempo de Vida (TTL) llegará a cero y no se hará ningún intento más de hacer la conexión.

Si los enrutadores encuentran el enrutador en que reside el host de destino, los paquetes circularán por la interfaz de red para ingresar al segmento LAN del host, utilizando la máscara de subred de la dirección IP de destino, si existe alguna.

El host receptor lee su mensaje y decide si debe responder. Para responder su solicitud de servicio, utiliza las técnicas de saludo TCP de tres vías y de ventaneo. Se establece la conexión y se ejecuta la solicitud de descargar la página Web bajo la administración de la técnica de ventaneo TCP.

En términos simplificados, esto es lo que pasa cuando se teclea un hipervínculo en un navegador.

PARTE II

Herramientas de Cisco para la interconectividad

CAPÍTULO 3

Revisión general de los enrutadores

La interconectividad requiere gran cantidad de hardware, software, medios de telecomunicación y experiencia técnica. Conmutadores, concentradores, firewalls, paquetes, compuertas, puertos, servidores de acceso, interfaces, capas, protocolos, líneas seriales, ISDN, marcos, topologías (la lista parece interminable). Sin embargo, existe un dispositivo indispensable en medio de todo esto. Una entidad única y tangible que mantiene los paquetes circulando en la dirección correcta: el enrutador.

En los términos más básicos, la interconectividad no se relaciona más que con la vinculación de computadoras y personas a través de un laberinto de dispositivos computacionales y dispositivos intermedios de telecomunicaciones. Esto es lo que se requiere para el enrutamiento; en esencia, realiza dos funciones: determina una ruta que permite establecer un vínculo y transmite paquetes a través de esa ruta. Es dentro de estas dos funciones (que se llevan a cabo en el interior del enrutador) que la conectividad se convierte en algo sencillo de comprender. Esto se debe a que el enrutador en sí debe reducir toda la complejidad a un nivel en que se pueda manejar. El enrutador lleva a cabo esta tarea trabajando con todo, de paquete IP en paquete IP.

Viéndolo de esta forma, el enrutador es la parte fundamental de las interconexiones. En realidad, sin el enrutador, no existiría Internet como lo conocemos ahora. Esto se debe a sus capacidades únicas y de gran poder:

- ▼ Los enrutadores soportan diferentes protocolos de manera simultánea (como Ethernet, Token Ring, ISDN y otros), haciendo que casi todas las computadoras sean compatibles en el nivel de la interconexión.
- ■ Los enrutadores conectan las redes de área local (LAN) con las de área amplia (WAN), lo que hace factible la construcción de interconexiones a gran escala con un mínimo de planeación centralizada (algo parecido a la serie Lego™).
- ■ Los enrutadores filtran el tráfico no deseado, aislando áreas en que los mensajes puedan ser "difundidos" a todos los usuarios de la red.
- ■ Pueden actuar como compuertas simples de seguridad verificando o "comparando" el tráfico con las listas de control de acceso (ACL, Access Control Lists).
- ■ Los enrutadores también aseguran la confiabilidad del transporte proporcionando trayectorias múltiples a través de las interconexiones.
- ▲ Se pueden configurar para que aprendan de manera automática nuevas rutas y seleccionen las mejores, eliminando así las restricciones artificiales en el cambio de interconexiones.

En otras palabras, los enrutadores hacen posibles las interconexiones. Y lo hacen al proporcionar un entorno unificado y seguro en que grandes grupos de personas pueden conectarse. Sin embargo, hay obstáculos para conectar a los usuarios mediante interconexiones, ya sea en una intranet corporativa, una red privada virtual o Internet. En la figura 3-1 se describe cómo la tecnología del enrutador es la clave para superar estos obstáculos.

La capacidad del enrutador para soportar las comunicaciones entre una gran variedad de dispositivos es, sin lugar a dudas, su papel más importante. Vayamos al pasado cuando la industria de la computación invirtió décadas y millones de dólares debatiendo cómo se iban a comunicar entre sí las computadoras. Todas las peleas, el posicionamiento y los problemas para hacer compatibles los diferentes sistemas de propietario tuvieron un éxito muy limitado. Sin embargo, en menos de una década, la interconectividad TCP/IP se convirtió

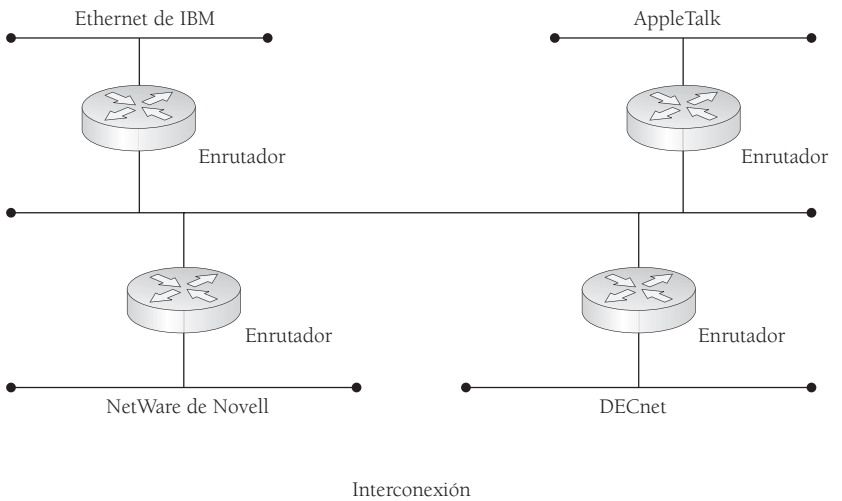


Figura 3-1. Los enrutadores hacen que las interconexiones sean una realidad superando los problemas de incompatibilidad.

en una plataforma común que permitió a casi todas las computadoras y arquitecturas de red intercambiar información libremente.

La capacidad de un enrutador para filtrar el tráfico remoto indeseable también es importante en la interconectividad. Si los usuarios fueran bombardeados con enormes volúmenes de mensajes indeseables o si sintieran que sus sistemas fueran fáciles de ser atacados por intrusos, se resistirían a estar conectados en red. El filtrado y control de acceso adecuadamente configurados que proporcionan los enrutadores pueden brindar a los usuarios (dispositivos) la protección básica necesaria para participar de manera eficiente en las interconexiones.

Existen otros tipos de dispositivos de red importantes, además del enrutador, pero la comprensión del funcionamiento del enrutador le ayudará de manera importante a comprender cómo funcionan las interconexiones. Sin embargo, antes de que aprenda cómo configurar y administrar los enrutadores, necesita conocer los fundamentos que los conforman. En este capítulo se ofrece un panorama general del hardware y software de los enrutadores Cisco.

CÓMO TRABAJAN LOS ENRUTADORES

En pocas palabras, los enrutadores hacen exactamente lo que su nombre indica: enrutan los datos de una red a otra y después a otra y así, hasta su destino final. Los enrutadores también actúan como agentes de tráfico, permitiendo que sólo computadoras autorizadas transmitan datos en la red local, de tal forma que la información confidencial pueda mantenerse segura. Los enrutadores se utilizan para soportar muchos tipos de conexiones de red, desde dedicadas, como Ethernet o líneas arrendadas, hasta conexiones de marcado

telefónico. Además de soportar estas conexiones, manejan errores y algunos problemas de seguridad, y mantienen estadísticas de uso de la red.

Enrutamiento para lograr mayor eficiencia

Cuando descarga un archivo de un servidor de protocolo de transferencia de archivos (FTP), es la tecnología de enrutamiento la que asegura que está obteniendo el archivo desde un servidor específico y no desde un servidor conectado a cualquier otro lugar en Internet. Los enrutadores dirigen el flujo de tráfico entre redes, en lugar de hacerlo dentro de éstas. Por ejemplo, examinemos cómo los enrutadores pueden utilizarse dentro de una red LAN para mantener el flujo de información.

Como se muestra en la figura 3-2, Design-O-Rama es una compañía de generación de imágenes por computadora. Su LAN está dividida en dos LAN más pequeñas (una para las animaciones y la otra para el grupo de administración y soporte). Las dos subdivisiones se conectan por medio de un enrutador. Design-O-Rama emplea ocho personas (cuatro del

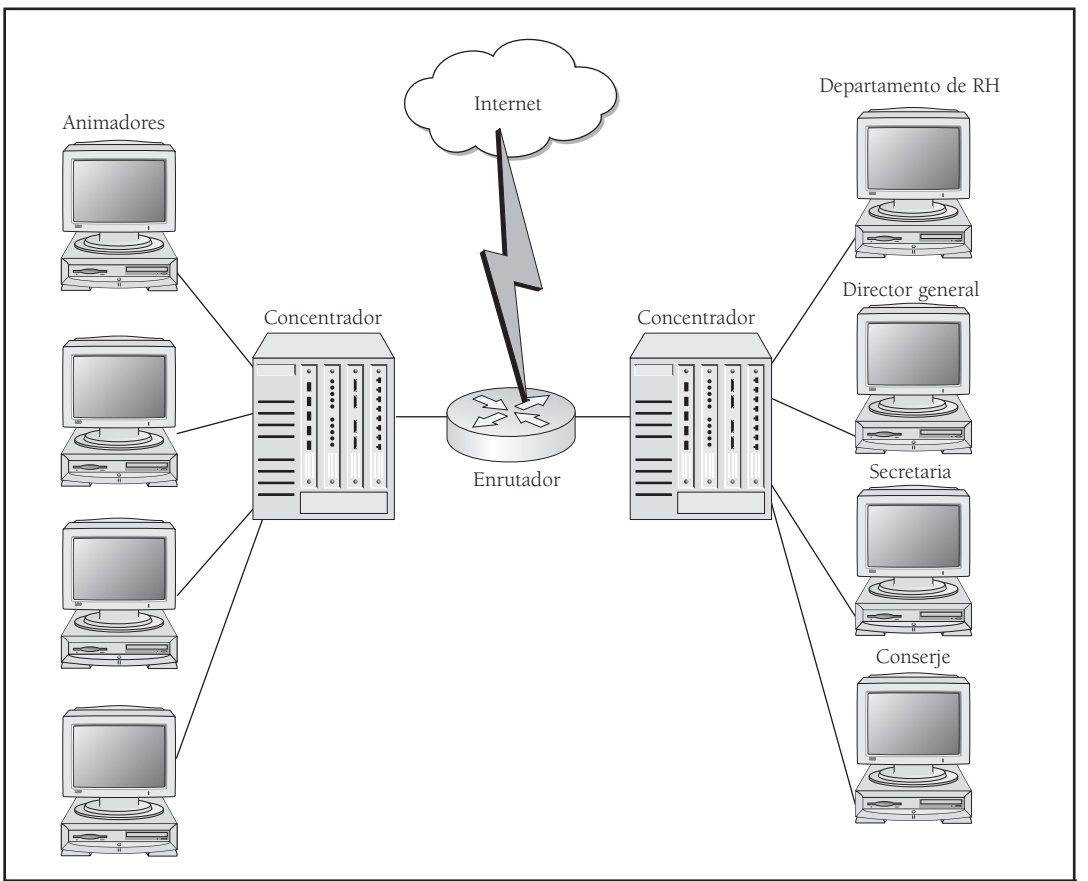


Figura 3-2. Los enrutadores pueden utilizarse para mejorar la eficiencia dentro de una LAN.

grupo de animación y cuatro del staff). Cuando un animador envía un archivo a otro animador, dicho archivo utilizará gran parte de la capacidad de la red. Lo anterior dará como resultado problemas de rendimiento para las demás personas conectadas en la red.

NOTA Recuerde cómo funciona Ethernet. Un solo usuario puede provocar un impacto muy grande en la red, porque cada paquete de información enviado por una computadora se difunde a todas las demás computadoras de la LAN. Entonces cada computadora examina el paquete y decide si fue dirigido a ésta.

Para evitar que los animadores reduzcan constantemente la velocidad de la red, ésta se divide en dos (una para los animadores y la otra para todos los demás). Un enrutador vincula las dos redes y las conecta a Internet. El enrutador es el único dispositivo en la red que ve cada mensaje enviado por cualquier computadora en cualquier red. Cuando un animador envía un archivo a un colega, el enrutador verifica la dirección del receptor y mantiene esa porción de tráfico aislada de esa LAN. Por otra parte, si el animador desea consultar con el departamento de Recursos Humanos información relacionada con sus vacaciones, el enrutador sabe que debe dirigir esos paquetes al segmento de red del departamento de Recursos Humanos.

Los enrutadores e Internet

En nuestro ejemplo anterior, analizamos cómo puede utilizarse localmente un enrutador. Ahora, ampliemos el panorama acerca de lo que hacen los enrutadores para incluir su funcionalidad en todo Internet.

Para comparar, hablemos primero acerca de cómo una llamada telefónica se enruta a través de un país. Digamos que es el cumpleaños de su tía Sandra y en lugar de enviarle un correo electrónico, quiere hablarle por teléfono. Cuando realiza una llamada, el sistema telefónico establece un circuito permanente entre su teléfono y el de la tía Sandra. Es probable que el circuito salte por varias etapas, incluidas fibras ópticas, alambre de cobre y satélites. Esta cadena de extremo a extremo asegura que la calidad de la línea entre usted y su tía Sandra será constante. Sin embargo, si el satélite queda fuera de línea o si un grupo de trabajadores rompe el cable de fibra óptica, su conversación con la tía Sandra se verá interrumpida. Internet evita este problema haciendo sus "llamadas" de una manera totalmente diferente.

Paquetes y rutas

Cualquier información que se envíe por Internet (correo electrónico, páginas Web, etcétera), ésta se fragmenta en paquetes. El tamaño de estos paquetes variará de acuerdo con los parámetros de la red y otros factores que se estudiarán más adelante (para este análisis, digamos que el tamaño es de 1 500 bytes). Los paquetes pueden transmitirse a través un determinado número de enrutadores, cada uno de los cuales envía el paquete hacia el dispositivo de destino. Los paquetes serán transmitidos a través de la mejor ruta disponible. Todos o ninguno de los paquetes pueden tomar la misma ruta. Una vez que los paquetes han llegado a la computadora de destino, se reensamblan. Este proceso se lleva a cabo tan rápido que usted ni siquiera sabrá que el archivo se fragmentó en paquetes de 1 500 bytes y, después, se volvió a ensamblar.

En la figura 3-3 se ilustra cómo funciona una red de conmutación en paquetes. Los enrutadores en Internet están conectados en forma de telaraña. Los paquetes siguen el camino de

menor resistencia para asegurar que lleguen a su destino en un espacio razonable de tiempo. Parece lógico que los paquetes recorran el menor número de enrutadores para llegar a su destino. Sin embargo, a veces la ruta más rápida no es siempre la más directa. Esto se debe a que puede haber un congestionamiento en la red o un vínculo lento en el "último salto" de la ruta más corta. Los enrutadores pueden enviar el tráfico alrededor de las porciones más congestionadas de Internet para aumentar la velocidad y la eficiencia.

Tal vez parezca un sistema complejo (comparado con el proceso que se sigue cuando se establece una llamada telefónica), pero el sistema funciona por dos razones importantes:

- ▼ La red puede equilibrar la carga entre diferentes equipos de un milisegundo a otro.
- ▲ Si se presenta un problema con un equipo de la red mientras se está transmitiendo un mensaje, los paquetes pueden enrutarse por otro camino, para asegurarse de que se reciba el mensaje completo.

Los enrutadores que conforman la espina dorsal principal de Internet pueden reconfigurar las rutas que toman los paquetes, porque ven toda la información que rodea al paquete de datos y se comunican entre sí la información relacionada con las condiciones de la línea, como la presencia de problemas para enviar y recibir datos en varias partes de Internet.

Todas las formas y tamaños

No todos los enrutadores son responsables del destino de los paquetes que circulan por Internet. Los enrutadores tienen tamaños diferentes y hacen más o menos, dependiendo de su tamaño y sofisticación. Por ejemplo:

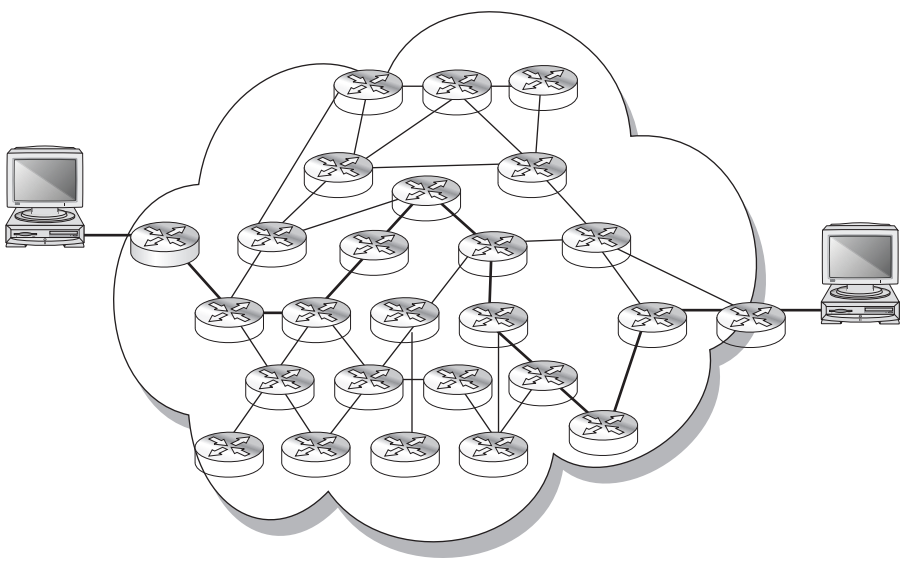


Figura 3-3. Los enrutadores envían los paquetes por la ruta que detectan que tiene la menor resistencia.

- ▼ Si tiene habilitada la función Compartir una conexión de Internet entre dos computadoras con Windows XP de Microsoft, la computadora conectada a Internet está actuando como un simple enrutador. Este enrutador hace muy poco: sólo revisa los datos para ver a qué computadora van dirigidos.
- ■ Los enrutadores que se utilizan para conectar pequeñas oficinas a Internet realizan más tareas. Estos pueden configurarse para que cumplan las reglas de seguridad de la LAN de la oficina, y suelen manejar el tráfico suficiente como para que estos enrutadores tienden a ser dispositivos independientes.
- ▲ Los enrutadores más grandes (los que se utilizan para manejar datos en los puntos de mayor tráfico de Internet) manejan gran cantidad de información (millones de paquetes por segundo). Se trata de dispositivos independientes que parecieran fabricados por una empresa de electrodomésticos más que de computadoras.

Consideremos el enrutador de tamaño medio (tal vez sea algo que está zumbando en un cuarto pequeño ubicado en un negocio de tamaño pequeño o mediano). Para simplificar, digamos que este enrutador sólo tiene que relacionarse con dos instancias (su LAN e Internet). La LAN de la oficina se conecta al enrutador por medio de una conexión Ethernet. Tal vez el enrutador también tenga dos conexiones hacia el ISP de su compañía (una conexión T3 y otra ISDN). Casi siempre, su tráfico va y viene por la línea T3. Sin embargo, la línea ISDN se utiliza en el caso de que algo salga mal con la línea T3. En realidad, el enrutador está configurado para enviar datos a través de la línea ISDN, porque se ha programado la tabla de configuración para conmutarse a la otra en caso de una emergencia.

Este enrutador también tiene otra función (puede ser una capa de "vigilancia" contra ataques externos). A pesar de que los firewalls suelen utilizarse para evitar accesos indebidos, y son muy recomendables (sería una locura que no utilizara uno cuando se conecta a Internet), también se debe configurar un enrutador externo con fines de seguridad.

La espina dorsal de Internet utiliza el tercer tipo de enrutador de la lista. El Gigabit Switch serie 12000 de Cisco es el tipo de equipo que se utiliza para trabajar con Internet. Estos enrutadores están diseñados y construidos como una supercomputadora. Por ejemplo, la serie 12000 utiliza procesadores a 200 MHz MIPS R5000, que son del mismo tipo que utilizan las computadoras que generan los efectos especiales en las películas. El enrutador más grande de Cisco (el 12816) maneja hasta 1.28 billones de bits de información por segundo.

Enrutadores ópticos

En una interconexión convencional, la información se transmitiría utilizando cable de cobre de par trenzado a través de una WAN o hasta una LAN. Aunque el cableado de alambre de par trenzado y la red eléctrica han sido muy útiles, la fibra óptica permite que la información se transfiera a velocidades inmensamente más elevadas. En el pasado, cuando las computadoras compartían conversaciones muy cortas, las redes eléctricas podían manejar esas cargas de tráfico. Sin embargo, en la actualidad, a medida que la información se comparte como nunca antes, se presenta una clara necesidad de actualizar la capacidad de la red.

Comparar las velocidades de transmisión de las redes eléctricas con las ópticas sería como poner a pelear a Woody Allen con Mike Tyson en el patio de una prisión (simplemente no hay punto de comparación). Las características más importantes de las redes ópticas son una gran velocidad y una capacidad enorme.

Los vínculos WAN comunes que se mueven a través de las redes eléctricas son T1 (1.544 Mbps) y T3 (45 Mbps). Del lado de las LAN, las cosas son más sencillas. Casi todas las organizaciones utilizan Ethernet a 10 o 100 Mbps. La Ethernet más moderna funciona a una velocidad de 10 Gbps. Sin embargo, una vez que entran a la carrera las fibra ópticas, cuidado.

En el extremo inferior, las redes de fibra óptica son más rápidas que un T1 o un T3. Una vez que la fibra cambia a segunda velocidad, deja de existir comparación. Cuando se analizan las velocidades de las redes ópticas, escuchará que la terminología cambia de T1 o T3 a OC. OC son las siglas en inglés de *portador óptico*. OC entra en juego cuando T sale de competencia. Una vez que el portador óptico sale a escena, las velocidades no sólo alcanzan 1 Gbps, sino que lo dejan muy atrás.

En la tabla 3-1 se muestra la forma en que aumentan las velocidades de línea de las redes ópticas.

Como observará, las velocidades de las redes ópticas (sin mencionar su desarrollo) han aumentado a una velocidad sorprendente. Gracias a la *multiplexión densa por división de longitud de onda (DWDM)*, el ancho de banda óptico sólo se incrementará, porque puede introducirse más de un flujo de datos en un solo tramo de fibra óptica. En un momento se hablará más al respecto.

Tecnologías ópticas

Son dos las tecnologías que prevalecen en el mundo del enrutamiento óptico: SONET y DWDM. SONET es la más antigua y popular, mientras que DWDM es la más novedosa, pero aporta capacidades mucho mayores que SONET. Analicemos estas tecnologías con mayor profundidad.

Designación	Velocidad
OC-1	51 Mbps
OC-3	155 Mbps
OC-12	622 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	9.952 Gbps
OC-768	40 Gbps

Tabla 3-1. Velocidades de redes ópticas.

SONET La arquitectura más básica y popular de una red óptica es la Red Óptica Sincrónica (SONET).

SONET es un estándar para el transporte de comunicaciones ópticas desarrollado por la Exchange Carriers Standards Association (ECSA) para el American National Standards Institute (ANSI), el organismo que establece los estándares industriales en Estados Unidos para telecomunicaciones y otras industrias. Se espera que el estándar SONET proporcione la infraestructura de transporte para las telecomunicaciones mundiales en las próximas dos o tres décadas, por lo menos.

NOTA En Europa, a SONET se le conoce con las siglas SDH, que es una abreviatura de Synchronous Digital Hierarchy.

SONET es tan veloz que puede transmitir un CD-ROM de 650 MB de Nueva York a Seattle en menos de un segundo. SONET no sólo es rápido, sino también muy versátil. Las llamadas de voz de una oficina a otra pueden multiplexarse junto con los datos a través de una sola fibra óptica. Más aún, debido a la enorme cantidad de ancho de banda con la que cuenta SONET, no es necesaria la compresión ni el encapsulado de los paquetes IP. Para efectos de comparación, una sola conexión OC-3 puede transportar más de dos mil llamadas simultáneas de voz. Además, es posible multiplexar todo tipo de datos junto con las llamadas.

SONET ofrece un ancho de banda máximo de OC-768 (39.813 Gbps) y puede transportar una gran variedad de información. Además de las grandes velocidades, las tasas de error de SONET son de 1 en 10,000 millones de bits. Compare esto con los métodos de transmisión por medio de cobre que tienen tasas de error de uno en un millón de bits.

DWDM En sus comienzos, SONET entregaba un ancho de banda que era imposible imaginar años antes. En ese entonces, la entrega de niveles OC-3 (155.52 Mbps) ofrecía más ancho de banda del que nadie sabía que hacer con él. Desde luego, eso sucedió a mediados de la década de 1980, una década antes de que aparecieran Internet y algunas aplicaciones de ancho de banda elevado. La tecnología se mantuvo entregando portadores ópticos cada vez más veloces. Después del OC-3, se fabricaron OC-12, OC-48 y más.

OC-192 (9.953 Gbps) es una velocidad popular en SONET; sin embargo, el nivel siguiente, OC-768 (39.813 Gbps), es la mejor calidad que SONET será capaz de entregar. Claro que hace diez años nadie sabía lo que era un gigabit, pero ahora lo sabemos y ya no nos es suficiente. El problema es que 40 Gbps está muy cerca del límite de SONET. La solución es saltar a DWDM.

DWDM es una técnica en que varias señales pueden viajar por una sola fibra óptica. Los láseres que se utilizan en las redes ópticas pueden sintonizarse a longitudes de onda diferentes (imagínelas como si fueran distintos colores). Como tales, es posible poner varios colores en una sola fibra. Cuando el enrutador receptor ve los diferentes colores, sabe qué colores separar para cada uno de los flujos de datos, como se muestra en la figura 3-4.

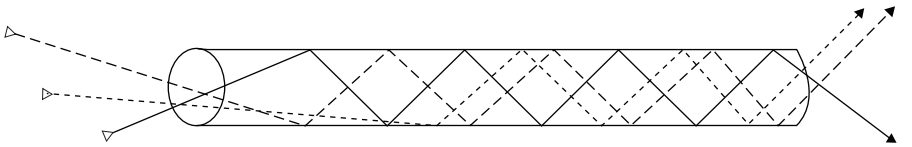


Figura 3-4. Pueden enviarse varias transmisiones a través de una sola fibra que utiliza DWDM.

Productos ópticos de Cisco

Cisco utiliza SONET y DWDM en sus enrutadores ópticos. Por ejemplo, el enrutador óptico ONS 15600 soporta tecnología SONET/SDH. Este enrutador de la clase de portador soporta velocidades de 40 Gbps y puede transmitir a una distancia de hasta 80 kilómetros.

Cisco también ofrece cierto nivel de modularidad en sus dispositivos. En vez de fabricar algunos modelos con un determinado número de puertos configurados para Gigabit Ethernet y otra cantidad dedicada a SONET o DWDM, la compañía ha desarrollado tarjetas y módulos que pueden conectarse en un enrutador, permitiendo que el cliente los configure. Es decir, puede decidir si instala el enrutador con módulos SONET, DWDM o cualquier combinación de módulos eléctricos y ópticos que desee.

COMUNICACIÓN CON UN ENRUTADOR

Casi ningún usuario de interconexiones se comunica con los enrutadores, se comunican *a través* de ellos. Sin embargo, los administradores de red deben trabajar directamente con enrutadores individuales para instalarlos y administrarlos.

Los enrutadores son computadoras construidas con un propósito específico dedicadas al procesamiento de las interconexiones. Son dispositivos importantes que, de manera individual, brindan servicio a cientos o miles de usuarios (algunos dan servicio a una cantidad aun mayor de usuarios). Cuando un enrutador falla, o su desempeño no es el adecuado, los usuarios se quejan y los administradores de red dan un salto. Como imaginará, los administradores de red requieren de formas a prueba de tontos para accesar a los enrutadores que administran y trabajar en ellos.

Los enrutadores no incluyen un monitor, un teclado o un ratón, por lo que puede comunicarse con ellos de una de las maneras siguientes:

- Desde una terminal que esté en el mismo lugar que el enrutador y que se encuentre conectada físicamente a él por medio de un cable de consola (la terminal suele ser una PC o estación de trabajo operando en modo terminal).

- Desde una terminal que se encuentra en un lugar diferente y que se conecta al enrutador por medio de un módem que llama a otro que está conectado al enrutador con un cable (por lo general, se conecta en el puerto auxiliar del enrutador).
- ▲ A través de la red en que se encuentra instalado el enrutador, utilizando software de emulación de terminal, como Telnet, SSH o consolas de administración basadas en Web que utilicen HTTP o HTTPS.

En redes grandes, los administradores de red suelen estar alejados físicamente de los enrutadores y deben acceder a ellos a través de una red. Sin embargo, si no puede acceder al enrutador por un problema en la red, o si no hay ningún módem conectado al enrutador, alguien debe ir adonde se encuentra y accederlo directamente. Existen tres formas de obtener acceso administrativo a los enrutadores, como se muestra en la figura 3-5.

Aunque los administradores de red administren los enrutadores ubicados en el mismo edificio, aún prefieren acceder a ellos a través de la red. Para muchas organizaciones, no tiene sentido tener una terminal conectada a cada enrutador, sobre todo cuando existen docenas de éstos apilados en un gabinete de datos o en un cuarto de computadoras. Además, es mucho más conveniente administrarlos todos desde una sola PC o estación de trabajo.

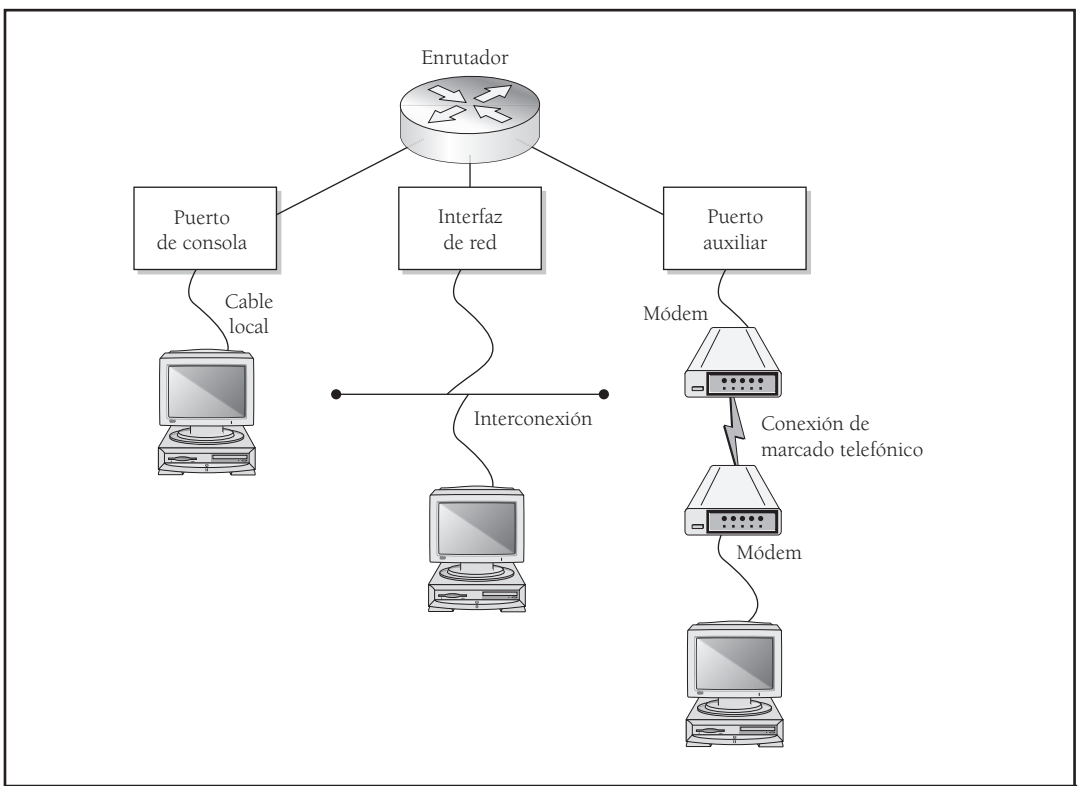


Figura 3-5. El acceso administrativo a los enrutadores se obtiene de tres maneras diferentes.

Hay varias formas de comunicarse con un enrutador, y cada una es posible a través de un protocolo de comunicaciones particular. En la tabla 3-2 se proporciona una lista en que se incluyen el método, el protocolo y la manera en que se utiliza cada uno.

El puerto de consola

Cada enrutador Cisco tiene un puerto para una consola. Está ahí para proporcionar una forma de conectar una terminal al enrutador para trabajar con él. Los administradores utilizan el puerto de la consola (llamada a veces puerto de administración) para ingresar directamente al enrutador (es decir, sin una conexión de red). La consola debe utilizarse para instalar enrutadores en redes, porque en ese punto no existe conexión de red que permita trabajar con ella.

A largo plazo, la función de la consola es estar ahí como contingencia en caso de una emergencia. Cuando un enrutador queda totalmente fuera de servicio (en otras palabras, cuando no puede procesar paquetes de red) no puede accederse a él mediante la red. Si el enrutador está funcionando y procesando paquetes, pero no trabaja el segmento de red que da acceso a él, no se cuenta con la opción de usar una red para arreglar el enrutador. Es cuando el puerto de consola proporciona una forma segura de acceder al enrutador para corregir los problemas, o cuando cuenta con un servidor de terminal especial configurado para permitir el acceso remoto.

Método de acceso	Protocolo	Método de comunicaciones
Puerto de la consola	EIA/TIA-232	Conexión serial en línea desde la terminal local.
Puerto auxiliar	EIA/TIA-232	Terminal serial en línea vía módem.
Telnet/Secure Shell (SSH)	Telnet/SSH	Conexión terminal virtual vía una red TCP/IP.
Servidor HTTP/HTTPS	HTTP/HTTPS	Conexión al navegador Web vía una red TCP/IP.
SNMP	SNMP	Protocolo simple de administración de la red; es una conexión de terminal virtual realizada a través de una red TCP/IP. (El protocolo SNMP se estudia en el capítulo 13.)

Tabla 3-2. Cómo acceden los administradores de red a los enrutadores.

Tipos de terminal de consola

Un cliente, una PC o una estación de trabajo independiente puede utilizarse como consola. Las terminales de consola deben ejecutar una interfaz de usuario basada en caracteres. No pueden ejecutar una interfaz gráfica de usuario (GUI), como Windows de Microsoft, Mac OS o X-Windows. Para utilizar una PC o estación de trabajo como consola, debe utilizar software de emulación de terminal. Por ejemplo, uno de los emuladores de terminal mejor conocidos es HyperTerminal, de Hilgraeve, Inc., que se entrega con todas las versiones de Windows. Inicie HyperTerminal (o uno de los muchos otros productos para emulación de terminal) y, desde ahí, ingrese al enrutador.

Tipos de conectores de consola

Los puertos de consola de los enrutadores Cisco utilizan una gran variedad de tipos de conectores (de 25 pines, RJ-45, de 9 pines, etcétera), pero todos ofrecen una conexión única de terminal. Una advertencia: asegúrese de contar con el cable flexible adecuado (que no sea cable Ethernet) antes de tratar de conectar una terminal de consola para que trabaje con un enrutador. Muchos administradores de red han pasado media hora probando cables distintos para encontrar uno que se pueda conectar a un enrutador sólo para realizar un trabajo productivo durante 15 minutos.

NOTA Los puertos de consola de los dispositivos Cisco suelen estar etiquetados como "Console" (pero no siempre). En algunos productos, los puertos de la consola tienen una etiqueta que dice "Admin", y en otros tiene una que dice "Management". No se deje confundir por esto; todos son puertos de consola.

El puerto auxiliar

Casi todos los enrutadores Cisco cuentan con un segundo puerto en la parte trasera llamado puerto auxiliar (suele llamarse puerto AUX, para abreviar). Al igual que el puerto de consola, el puerto AUX hace posible una conexión directa, que no es de red, al enrutador.

¿Cuál es la diferencia entre el puerto AUX y el de consola? El puerto AUX utiliza un tipo de conector al que pueden conectarse los módems (los puertos de consola cuentan con conectores diseñados para los cables de terminales). Si falla un enrutador ubicado en un gabinete de datos lejano, el administrador de la red solicita a alguna persona del área que vaya al enrutador y conecte un módem para que pueda proporcionarle servicio de manera remota. En configuraciones más críticas, con frecuencia se deja un módem conectado de manera permanente a un puerto AUX del enrutador. De cualquier forma, el puerto AUX permite el acceso tipo consola cuando no es práctico enviar a un técnico al sitio a trabajar en un enrutador mediante una consola local.

En la figura 3-6 se muestran los puertos AUX y de consola en la parte trasera de un enrutador Cisco 4500.

NOTA Los enrutadores más pequeños de Cisco no cuentan con puertos AUX; sólo con puertos de consola. Estos dispositivos soportan acceso para administración remota conectando un módem al enrutador con un kit de cables auxiliar/consola.

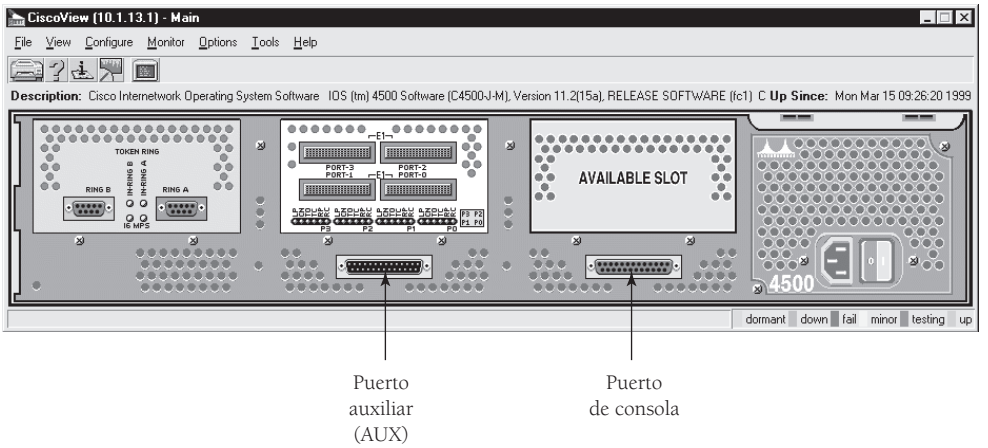


Figura 3-6. Los puertos AUX y de consola de un enrutador 4500 de Cisco permiten conexiones directas, sin utilizar la red.

Telnet

Una vez que se instala un enrutador en una red, el acceso a éste se lleva a cabo casi siempre mediante una conexión Secure Shell (SSH) o una sesión Telnet sin codificar, no mediante los puertos AUX y de consola. La persona más consciente de la seguridad preferiría una conexión SSH, y ésta deberá utilizarse cuando se acceda a un dispositivo mediante una red no confiable (que es prácticamente cualquier red, en cuanto al tipo de administración que uno hace con una parte de la infraestructura de red). En esta sección, utilizaremos el término Telnet, pero en el análisis todo se puede aplicar también a SSH, puesto que es, en esencia, una forma segura de Telnet. Esta conectividad es simplemente una forma de acceder a un enrutador como terminal virtual. Aquí la palabra "virtual" significa que no se crea una conexión de terminal real al dispositivo mediante un cable directo o un módem, como con los puertos de consola o AUX. En lugar de eso, las conexiones Telnet se hacen a través de la red. En términos muy sencillos, la sesión de terminal real se compone de flujos de bits enviadas de uno en uno a través de una línea serial. Una sesión de terminal virtual se compone de paquetes IP que se enrutan mediante una red, pretendiendo que son flujos de bits que viajan a través de una línea serial.

Telnet es una aplicación (no un emulador) de red. Se desarrolló en los primeros días del sistema operativo UNIX, como una forma de acceder a computadoras remotas para administrarlas. Más adelante, los pioneros de las interconexiones incorporaron Telnet directamente en el protocolo de conectividad TCP/IP como una forma de acceder y administrar dispositivos de conectividad. Un cliente y servidor Telnet se entrega con cada copia del software IOS de Cisco y casi todos los sistemas operativos para computadora.

Cuando se utiliza Telnet para acceder a un enrutador, lo hace a través de una línea virtual proporcionada por el software IOS de Cisco. A éstas se les denomina *líneas VTY*. No permita que la palabra "línea" lo confunda. No se refiere a un circuito real de comunicacio-

nes; significa una sesión de terminal virtual dentro del software IOS. El IOS soporta hasta cinco líneas terminales virtuales (numeradas VTY 0-4, incluidas), lo que permite que hasta cinco sesiones de terminal virtual funcionen en un enrutador al mismo tiempo. Sin embargo, esto es una exageración en el diseño. Es poco común tener al mismo tiempo más de una sesión de terminal virtual en un enrutador. Algunos enrutadores cuentan con más de cinco líneas VTY y, con la versión Enterprise del IOS, puede asignar aún más.

El software IOS de Cisco se utiliza principalmente en modo de interfaz basada en caracteres, lo que significa que no es un ambiente GUI de apuntar y hacer clic, como el que acostumbramos utilizar en nuestras PC de Microsoft Windows, Apple Mac o estaciones de trabajo UNIX de X-Windows. Ya sea que inicie sesión en un enrutador mediante el puerto de consola, el puerto AUX o Telnet, está entrando en contacto con la interfaz de software IOS basada en caracteres. A continuación se muestra una salida de IOS basada en caracteres:

```
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 2
 exec-timeout 0 0
 password 7 1313041B
 login
line vty 3
 exec-timeout 5 0
 password 7 1313041B
 login
line vty 4
 exec-timeout 0 0
 password 7 1313041B
 login
!
```

El ejemplo anterior muestra las siete líneas IOS (*con* para consola, *aux* para auxiliar y *vty* para terminal virtual). Las siete líneas son:

- ▼ El puerto de consola, accesado por medio de una conexión local por cable.
- ■ El puerto AUX, accesado mediante una conexión de módem.
- ▲ Las cinco líneas VTY, accesadas mediante conexiones de red TCP/IP.

La interfaz de usuario del servidor HTTP

Un método de acceso a enrutadores más reciente es HTTP Server. Que el nombre no lo confunda; ningún servidor de computadora interviene en el uso de HTTP Server. El "servidor" en HTTP Server se refiere a una pequeña aplicación de software que funciona dentro del software IOS de Cisco. HTTP Server estuvo disponible por primera vez en la versión 10.3 de

IOS. HTTP Server permite interactuar con el enrutador mediante un navegador Web. En la figura 3-7 se muestra una pantalla HTTP Server.

Como tantos dispositivos y aplicaciones de Cisco, sus aplicaciones de usuario tienden a cambiar con el tiempo. Su interfaz de dispositivo quizás tenga la apariencia que se muestra en la figura 3-7. Es decir, se presentará la misma funcionalidad básica. Sólo que estará accesible mediante una interfase ligeramente diferente.

No es muy ergonómico utilizar HTTP para manejar la entrada y salida de la línea de comandos del IOS. La mayoría de los administradores de red aún prefieren utilizar el software IOS en el modo basado en caracteres, porque es más rápido y más directo que apuntar y hacer clic. No es diferente a las manos que aparecen en la ventana del MS-DOS de Windows de Microsoft para teclear comandos en el nivel del sistema, pero Cisco actualizará el IOS de manera gradual hacia una interfaz gráfica de usuario por dos razones. La razón más obvia para ofrecer por lo menos una opción basada en GUI para trabajar con el IOS es que cada

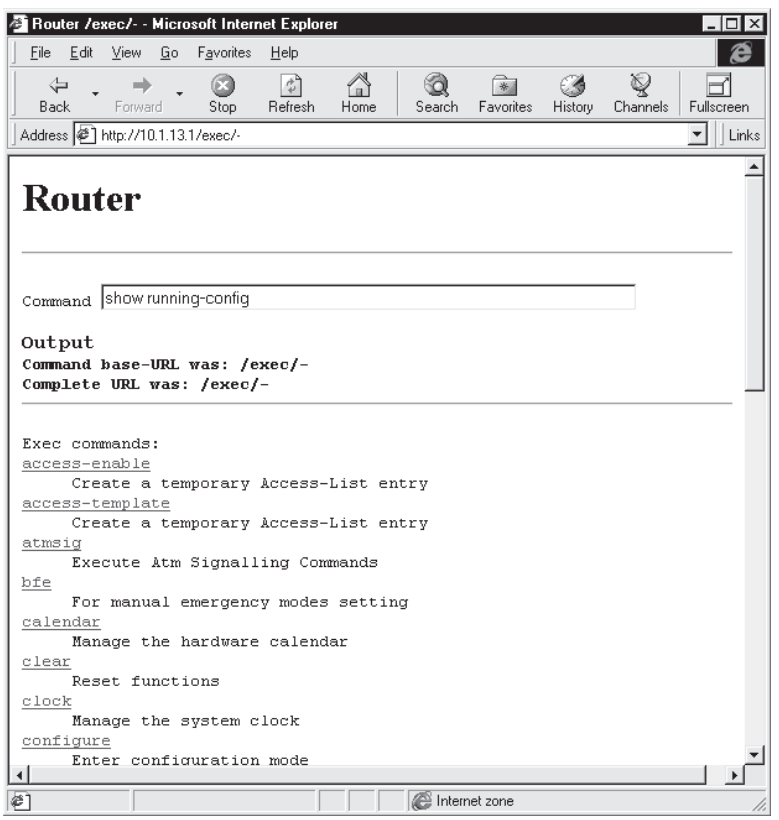


Figura 3-7. El IOS de Cisco se administra mediante una pantalla de HTTP Server.

vez son más los usuarios no expertos a los que están dirigidos los dispositivos de Cisco. La otra es que a medida que la complejidad aumenta, la necesidad de visualizar el sistema, aún dentro de un solo enrutador, se incrementa. El empleo de herramientas de visualización (para mostrar las condiciones de la carga, aislar errores, etcétera) requerirá, desde luego, un navegador en lugar de la interfaz "en pantalla verde" tradicional de línea de comandos basada en caracteres.

NOTA Para utilizar la interfaz de línea de comandos, debe saber cuáles comandos teclear. Quizás desee utilizar HTTP Server para comenzar y cambiar al modo basado en caracteres conforme se sienta más a gusto con la estructura de comandos del IOS.

Administrador de dispositivos de seguridad

Cisco Router and Security Device Manager (SDM, Router de Cisco y Administrador del dispositivo de seguridad) es la herramienta más reciente para la administración de dispositivos incrustados. El acceso se maneja por medio de una conexión SSL o SSH, para asegurar la comunicación entre la interfaz de usuario basada en Web y el dispositivo que se está administrando. Lo mejor de todo es que se puede descargar sin costo y trabaja con casi todos los enrutadores soportados. En los enrutadores más actuales, como el 850/870 y los modelos 1800, 2800 y 3800, ya está instalado y listo para usarse en cuanto lo saca usted de su caja.

Para facilitarle la vida, Cisco Router and Security Device Manager ofrece lo que Cisco llama "asistentes inteligentes basados en tareas", para ayudar con todo, desde la configuración inicial hasta configuraciones WAN/LAN y de seguridad más complicadas. Es un paso lógico en la administración de dispositivos para negocios pequeños y medianos, y también es útil en ambientes de sucursales de grandes corporativos, donde CiscoWorks sería la herramienta para la administración de la configuración y Cisco Router and Security Device Manager se utilizaría para reparar fallas o permitir el acceso de sólo lectura al dispositivo por parte del personal local. Este software puede encontrarse en www.cisco.com/go/sdm, junto con información adicional.

SDM también utiliza conexiones SSL y SSH para permitir que los administradores configuren enrutadores fácilmente de manera remota.

Cuando inicia SDM, podrá observar una pantalla como la que se muestra en la figura 3-8, que proporciona un resumen rápido del *status* de su enrutador. En ella se incluye lo siguiente:

- Modelo.
- Memoria disponible.
- Capacidad de memoria flash.
- Versión del IOS.
- Versión del SDM.
- Qué características se encuentran disponibles en su enrutador (como VPN, firewall, etcétera).
- Información acerca de la interfaz y la configuración de la conexión.
- Información de la configuración de firewall.

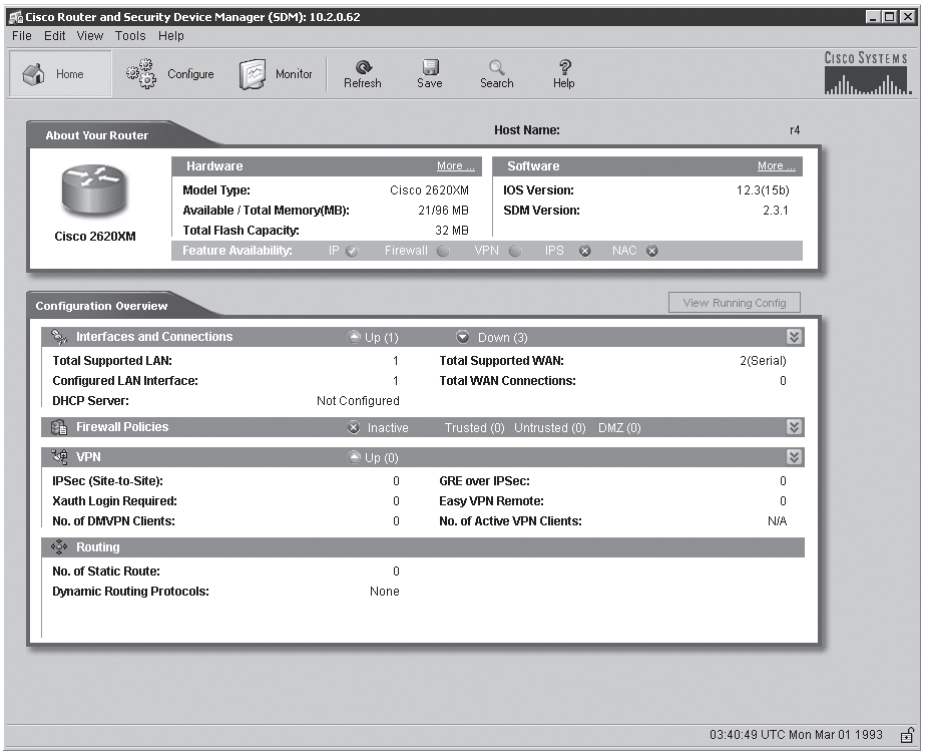


Figura 3-8. La página de inicio de SDM muestra un resumen con la información del enrutador.

- ■ Información de la configuración de VPN.
- ▲ Información del enrutamiento.

Asistentes inteligentes

Los asistentes inteligentes se utilizan en SDM para ayudar a configurar las diferentes características de su enrutador Cisco. Estos asistentes son útiles porque puede configurar dichas características con sólo apuntarlas y hacer clic, en lugar de tratar de recordar el comando correspondiente.

La manera como se inician los asistentes es la misma que se usa en una infinidad de asistentes con los que probablemente ha trabajado en un sistema Windows. Por ejemplo, para configurar la línea serial, iniciamos el WAN Wizard (Asistente para WAN). La pantalla se muestra en la figura 3-9.

Figura 3-9. SDM ayuda en el proceso de configuración proporcionando varios asistentes, como el WAN Wizard.

Una vez que hemos seleccionado la interfaz que deseamos configurar (en este caso, la línea serial) se nos dirige a otra página, que nos pregunta qué tipo de encapsulamiento deseamos configurar. Como se muestra en la figura 3-10, se proporcionan las opciones para elegir entre Frame Relay, protocolo punto a punto o control de vínculo de datos de alto nivel.

Después de seleccionar el tipo de encapsulamiento, el sistema nos lleva a otra pantalla, que se muestra en la figura 3-11 y que nos solicita la dirección IP y la máscara de la subred de la conexión.

Una vez que el asistente ha terminado de recolectar la información que usted proporcionó, envía sus selecciones e instrucciones a un archivo de configuración para el enrutador.

La línea de comandos también tiene una función en todo esto. En realidad, una vez que configure su enrutador o una característica de él, SDM convierte en código IOS lo que usted ha señalada y sobre lo que ha hecho clic después.

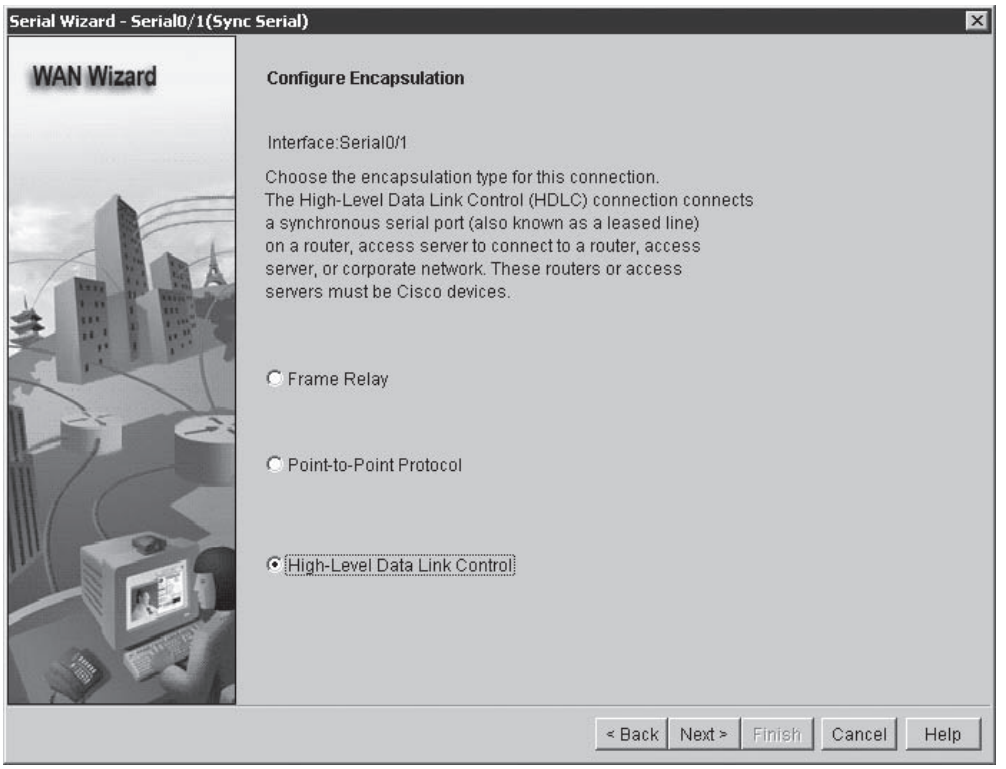


Figura 3-10. Seleccione el tipo de encapsulamiento que mejor satisfaga sus necesidades.

Monitoreo y detección y solución de problemas

SDM también le permite monitorear su enrutador para que pueda observar el valor de los parámetros en tiempo real. Por ejemplo, la pantalla que se muestra en la figura 3-12 presenta una gran cantidad de detalles de mucha utilidad. Podemos analizar el uso de la CPU, la memoria total, además de la memoria flash utilizada. Más aún, podemos analizar el *status* de cada conexión, lo que nos muestra si está funcionando o no y cuánto ancho de banda se está utilizando.

Para obtener aún más de una interfaz, al seleccionar y hacer clic en Interface Status (Estado de la interfaz), en la columna izquierda de iconos, se despliega una herramienta de rastreo que le permitirá monitorear ciertos detalles como:

- Los bytes que entran y salen.
- Los paquetes que entran y salen.

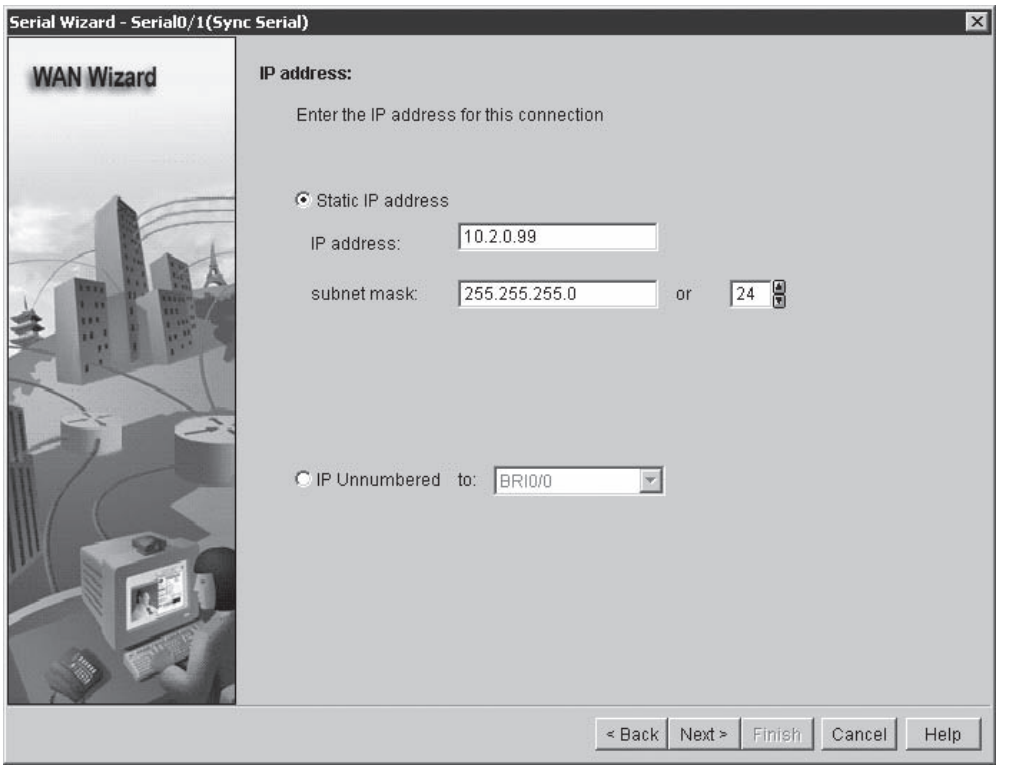


Figura 3-11. Solicita la dirección IP y la máscara de la subred de la conexión.

- Los errores.
- El uso del ancho de banda.

Esta herramienta se muestra en la figura 3-13.

Configuración del firewall

SDM también le permite configurar rápidamente un firewall en su enrutador. El Firewall Wizard (Asistente para firewall) lo lleva de la mano a dar los pasos necesarios para implantar diferentes niveles de seguridad.

Otra característica de SDM es la Router Security Audit (Auditoría de seguridad del router). Cuando accede a esta herramienta, SDM analiza la configuración de su enrutador y le informa dónde es necesario reforzar la seguridad. En la figura 3-14 se muestra un ejemplo.

Una vez que esta herramienta ha examinado su enrutador e identifica cualquier debilidad, puede checar puntos individuales, los cuales se corregirán automáticamente a través de SDM.

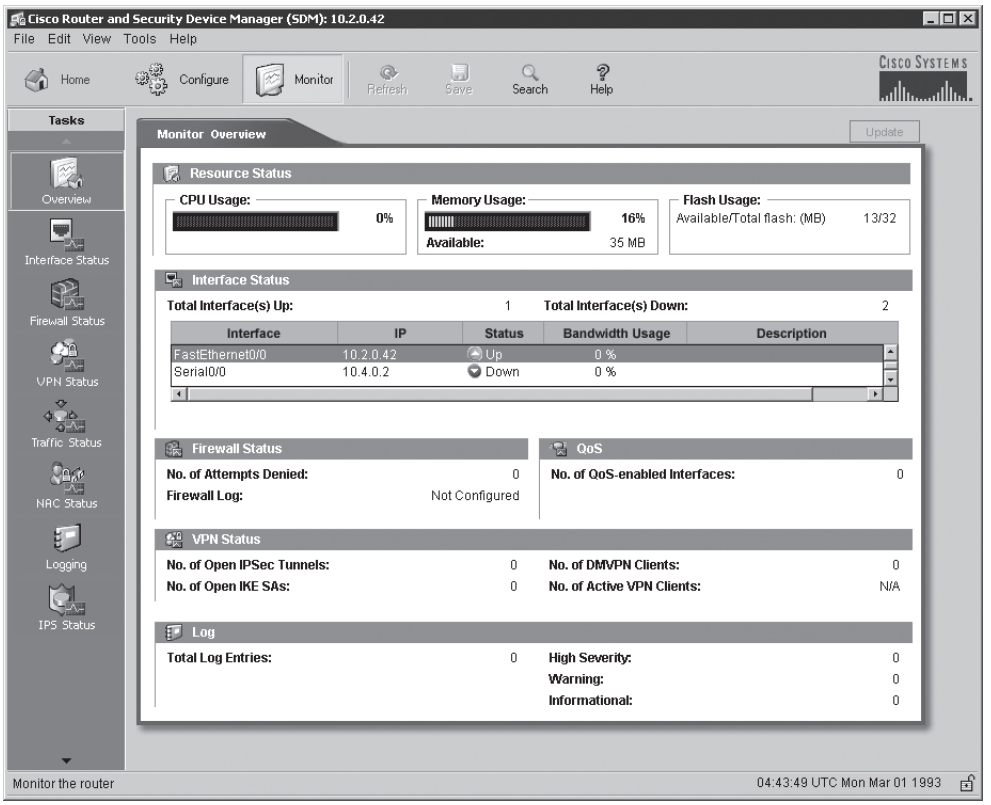


Figura 3-12. El SDM permite la supervisión de varios detalles del enrutador.

SEGURIDAD DE LOS ENRUTADORES

Los enrutadores que integran las redes no son muy visibles, sobre todo porque no suelen contar con direcciones, como www.yahoo.com o www.amazon.com. Los enrutadores no necesitan contar con direcciones amigables, porque los usuarios regulares de las redes nunca necesitan saber que ahí se encuentra un enrutador; sólo necesitan la conectividad que les proporciona.

Las únicas personas que necesitan acceder a un enrutador directamente son los miembros del grupo responsable de administrar la red. En las redes TCP/IP (el protocolo con el que trabaja la mayor parte de las redes) los enrutadores sólo se identifican a sí mismos ante las redes por medio de sus direcciones IP. Por esta razón, para acceder a un enrutador primero debe saber que existe y, después, saber cuál es su dirección IP. Desde luego, los administradores de red responsables del enrutador deberán saber está información.

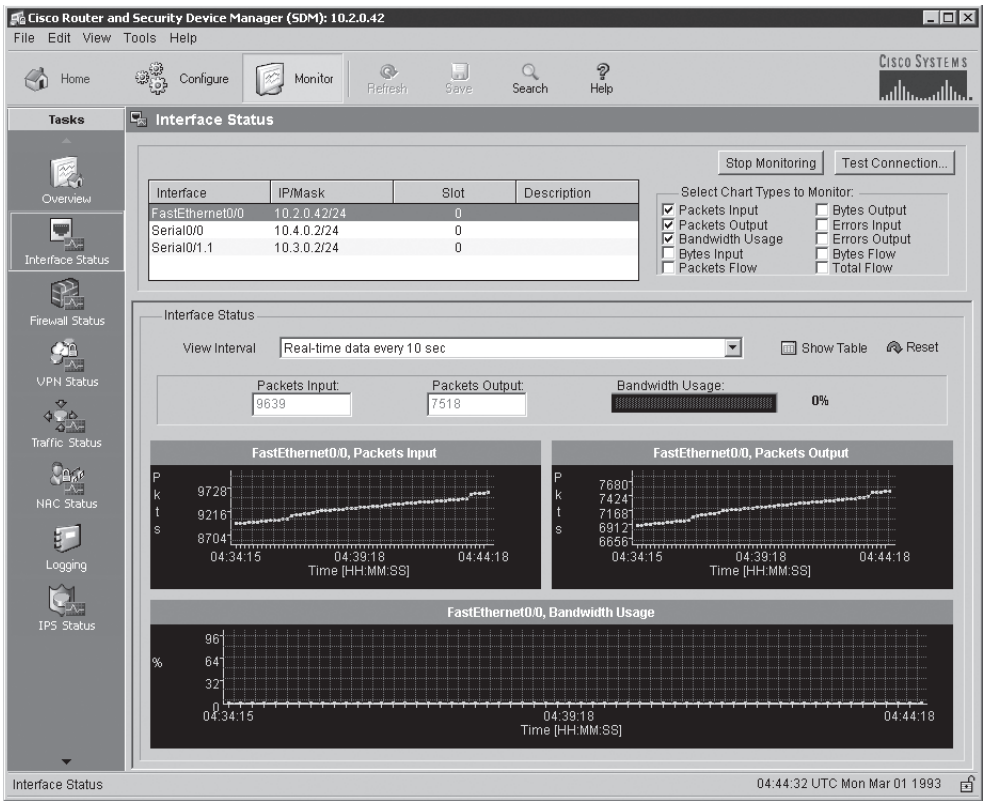


Figura 3-13. La herramienta Interface Status le permite rastrear las estadísticas de la interfaz.

Aún existe el problema potencial del abuso por parte de hackers. Como aprenderá en el capítulo 13, los enrutadores constantemente se envían mensajes entre sí con la finalidad de actualizar y administrar las redes en que operan. Con las debidas habilidades y una determinación suficiente, un hacker podría descubrir una dirección IP de un enrutador y, después, tratar de establecer una conexión Telnet con él. Dado que los enrutadores son los vínculos que mantienen unidas a las interconexiones, es fácil comprender por qué Cisco y otros fabricantes de equipo de conectividad diseñan muchas medidas de seguridad en sus productos. Como se muestra en la figura 3-15, la seguridad debe restringir el acceso a ciertas áreas dentro de una interconexión y a los dispositivos individuales.

NOTA Las contraseñas de los enrutadores sólo controlan el ingreso a los propios dispositivos. No confunda las contraseñas del enrutador con las que los usuarios regulares de una red deben teclear para acceder a ciertos sitios Web o a intranets (redes privadas). Las

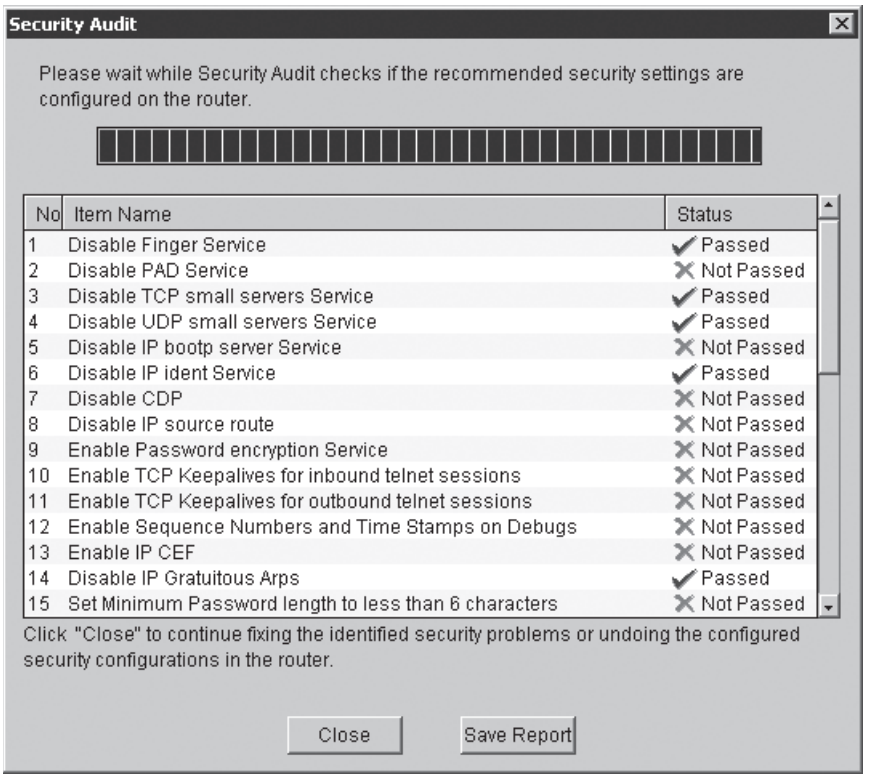


Figura 3-14. La herramienta Router Security Audit analiza la configuración de la seguridad del enrutador.

restricciones que se imponen a los usuarios regulares se administran por medio de firewalls y listas de acceso, que se estudian en el capítulo 14.

Contraseñas de enrutadores

La finalidad de las contraseñas de los enrutadores no es sólo evitar la presencia de hackers. Con frecuencia, la protección mediante contraseña se administra enrutador por enrutador. Aunque existe una gran variedad de métodos para la autenticación que permiten la administración centralizada de contraseñas, a menudo las contraseñas para acceder a un enrutador son "locales" en casi todas las implementaciones de tamaño pequeño o mediano. Esto significa que el nombre y la contraseña de usuario necesarios para acceder administrativamente al enrutador se almacenan dentro del propio enrutador. Las redes de gran tamaño que cuentan con docenas o cientos de enrutadores (algunos con operaciones de red más críticas que otros) pueden utilizar una solución administrada en forma central. Aún así, tal vez haya contraseñas locales, por lo que es una práctica común que los administradores de

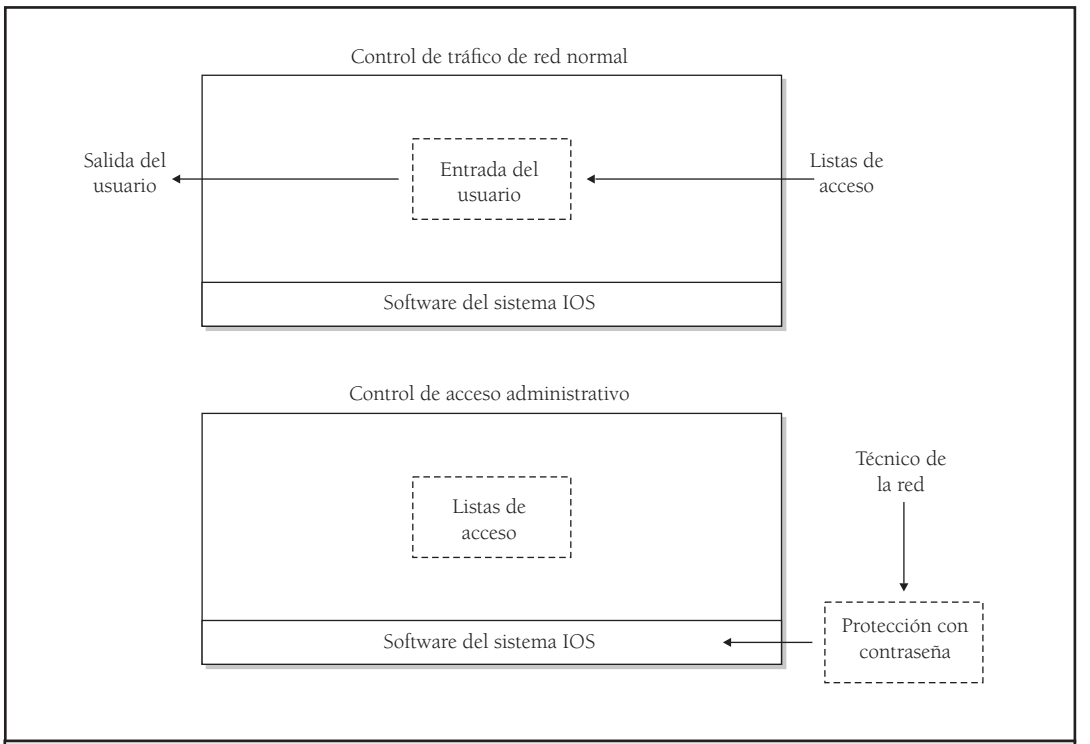


Figura 3-15. El control de la seguridad se administra de forma separada para el tráfico de la red y para el acceso administrativo.

redes sólo permitan el acceso a ciertos enrutadores o niveles de comando dentro de los enrutadores a determinados miembros del equipo de redes. En la tabla 3-3 se proporciona una lista de contraseñas de red y se indica lo que hacen.

En los enrutadores Cisco, las contraseñas se utilizan para controlar el acceso a:

- ▼ El propio dispositivo enrutador.
- ■ La porción EXEC privilegiado (modo de habilitación) del ambiente de software del IOS.
- ▲ El uso de comandos específicos del IOS.

Contraseñas de línea

Las contraseñas de línea se utilizan para controlar quién puede acceder al enrutador y también para establecer una contraseña en la línea terminal de la consola, en la línea AUX (auxiliar) y en cualquiera de las cinco líneas de terminal virtual (VTY), o en todas ellas.

Debe configurar por lo menos una contraseña para las líneas VTY del enrutador. Si no se configura una contraseña de línea, cuando intente acceder a un enrutador a través de Telnet, lo detendrá un mensaje de error, indicando que se "requiere contraseña pero no está establecida". Recuerde que cualquier persona en Internet puede usar Telnet con cualquier

Punto de control	Tipo de contraseña	Qué está restringido
Puerto de consola	Línea	Acceder a un enrutador vía una línea local conectada por medio del puerto de la consola.
Puerto AUX	Línea	Acceder a un enrutador vía una línea de módem (local) conectada vía el puerto auxiliar.
Acceso a la red	Línea	Acceder al enrutador vía una conexión de red utilizando Telnet o una línea VTY.
EXEC Privilegiado	Enable o Enable Secret	Acceder al nivel más potente de EXEC privilegiado del ambiente IOS.

Tabla 3-3. Panorama de las contraseñas de enrutador y sus usos.

enrutador, por lo que el establecimiento de contraseñas de línea evitará que todos los hackers obtengan acceso, con excepción de los más expertos. Aquí, el IOS está solicitando una contraseña:

```
User Access Verification

Password:
Router>>
```

Cuando ingrese contraseñas en el IOS, no aparecerán asteriscos para enmascarar las letras tecleadas, algo a lo que la mayoría de nosotros estamos acostumbrados. En el ejemplo anterior, en la solicitud Router>> (el nombre de host del enrutador en este ejemplo), se ingresó la contraseña correcta, el enrutador host accedió con éxito, pero no aparecieron asteriscos a la derecha de la solicitud de contraseña. Al principio, quizás esto lo desconcierte, sin embargo se acostumbrará.

NOTA Habrá notado que los ejemplos de contraseñas en este capítulo no se han hecho específicas de una persona con los nombres de usuario. Aunque es posible tener nombres de usuario con contraseñas Enable y Enable Secret, esto se hace con muy poca frecuencia. Esto se debe a que las contraseñas Enable y Enable Secret se almacenan en los archivos de configuración del enrutador. Aunque el uso de contraseñas compartidas representa un riesgo compartido y puede complicar la administración general de la red,

en caso de que alguien que conozca la contraseña se marche, aún podemos ver a muchos administradores de red que generan contraseñas genéricas para evitar el gran problema administrativo que representa mantener nombres y contraseñas de usuarios en docenas o cientos de enrutadores. Para abordar este tema con más detalle, por favor consulte el capítulo 6, donde se explica cómo pueden mantenerse centralmente las cuentas de usuario y las contraseñas utilizando TACACS+ y el servidor de control de acceso CiscoSecure.

Contraseñas Enable y Enable Secret

Una vez que haya pasado la contraseña de línea, habrá obtenido acceso al entorno de software del IOS. El IOS se divide en dos niveles privilegiados: EXEC y EXEC privilegiado (que suele denominarse modo de habilitación).

El nivel EXEC contiene solamente comandos básicos, no destructivos. Al estar en modo de habilitación se proporciona acceso a más comandos. En esencia, los comandos en EXEC le permiten ver tipos de información de diagnóstico acerca del enrutador. Los comandos en modo de habilitación son más poderosos, porque le permiten configurar los parámetros del enrutador. Estos comandos cuenta con la posibilidad de ser destructivos; el comando **erase** es un buen ejemplo.

Se pueden utilizar dos tipos de contraseña para restringir el acceso a EXEC privilegiado (modo de habilitación): Enable y Enable Secret. La idea de una "contraseña secreta" parece un poco tonta al principio. *Desde luego*, todas las contraseñas son secretas, o al menos deben serlo. A lo que los ingenieros de Cisco se refieren aquí es al nivel de codificación utilizado para enmascarar la contraseña de usuarios no autorizados.

El nivel EXEC privilegiado del IOS Las contraseñas Enable y Enable Secret hacen lo mismo: restringen el acceso al EXEC privilegiado (modo de habilitación). La diferencia entre los dos es el nivel soportado de codificación. La *codificación* es una técnica que se utiliza para mezclar datos de manera aleatoria, haciéndolos incomprensibles para quienes no cuenta con la clave para leerlos. Las contraseñas Enable Secret se cifran con un algoritmo avanzado de 128 bits, para lo que no se conoce una técnica de descifrado. El cifrado de la contraseña Enable depende de un algoritmo menos poderoso. Cisco definitivamente recomienda el uso del Enable Secret en lugar de Enable.

Enable Secret se presentó en 1997, de modo que aún se usa una buena cantidad de hardware y software que sólo soporta las contraseñas Enable, y los servidores que almacenan las imágenes de respaldo del IOS suelen proporcionar servicio tanto a enrutadores antiguos como nuevos. Cuando ambos están configurados, la contraseña Enable Secret siempre va primero que la Enable. El IOS solamente utilizará la contraseña Enable cuando esté funcionando una versión vieja del software IOS.

Las contraseñas IOS se almacenan en el archivo de configuración de un enrutador. Por lo general, los archivos de configuración circulan por las redes a medida que los enrutadores se actualizan y respaldan. El hecho de tener una contraseña Enable Secret significa que un hacker que utilice un analizador de protocolos (un dispositivo que lee paquetes) se enfrentará a una enorme cantidad de problemas si quiere descifrar su contraseña. El siguiente archivo de configuración ilustra lo anterior:

```
version 12.4
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$C/q2$ZhtujqzQIuJrRGqFwdwn71
enable password 7 0012000F
```

Observe que la máscara de cifrado de la contraseña Enable en la última línea, es mucho más corta que la máscara de codificación de la contraseña Enable Secret (de la segunda a la última línea).

NOTA Como estas contraseñas se almacenan de manera cifrada en el enrutador, los hackers corporativos han fabricado sus propias utilerías de software para obtener estas contraseñas. Programas como "Caín y Abel" le permiten a una persona ingresar la contraseña cifrada en la aplicación y, después, obtener la contraseña descifrada.

El comando para el servicio de codificación de contraseñas Ciertos tipos de contraseñas, como las de línea, aparecen de manera predeterminada en formato de texto en el archivo de configuración. Por tanto, debe evitar su uso. Puede utilizar el comando **service password-encryption** para hacerlas más seguras. Una vez que se ingresa este comando, cada contraseña configurada se codifica automáticamente y, por tanto, se hace ilegible dentro del archivo de configuración (de la misma manera que las contraseñas Enable/Enable Secret). El aseguramiento de las contraseñas de línea es doblemente importante en las redes en que se utilizan los servidores TFTP, porque el respaldo TFTP implica la transferencia rutinaria de los archivos de configuración a través de la red (y estos archivos contienen contraseñas de línea, desde luego).

EL HARDWARE DEL ENRUTADOR

A primera vista, los enrutadores se parecen mucho a una PC. Tienen una CPU; memoria; y, en la parte de atrás, puertos e interfaces para conectar periféricos y diferentes medios de comunicación. En ocasiones cuentan con un monitor para trabajar como una consola del sistema.

Sin embargo, existe una diferencia con una PC: los enrutadores no tiene disco; ni siquiera cuentan con unidades de discos flexibles. Si lo piensa, esto tiene sentido. Los enrutadores sólo sirven para enrutar, no para crear o desplegar los datos que transportan. Los enrutadores tiene la única misión de realizar la tarea de filtrado de los paquetes entrantes y enrutarlos hacia sus destinos.

Otra diferencia consiste en el tipo de módulos independientes que pueden conectarse a los enrutadores. Mientras que la típica PC contiene tarjetas para video, sonido, gráficos u otros propósitos, los módulos que se colocan en los enrutadores son estrictamente para conectividad (por razones obvias). Se les denomina *módulos de interfaz* o solamente *interfaces*. Cuando la gente o los documentos se refieren a una interfaz de enrutador, aluden a la tar-

jeta física de circuitos impresos que maneja un determinado protocolo de conectividad. Por ejemplo, E0 y E1, tal vez representen los números de interfaz de Ethernet 1 y 2 dentro de un enrutador. Hay un protocolo por interfaz.

Las interfaces se agregan de acuerdo con el entorno de red en que trabajarán. Por ejemplo, tal vez un enrutador sólo esté configurado con módulos de interfaz para Internet. Un enrutador que sirve en un entorno LAN combinado, en contraste, podría tener interfaces para los protocolos Ethernet y Token Ring, y si dicho enrutador estuviera trabajando como un vínculo LAN a WAN, también tendría un módulo ISDN.

Memoria del enrutador

Los enrutadores utilizan diferentes tipos de memoria para operar y administrarse a sí mismos. Existen muchas variaciones en la apariencia de la parte interna de un enrutador (con base en lo que hacen y cómo lo hacen). En la figura 3-16 se muestra el esquema de la tarjeta madre de un enrutador Cisco. Éste es un clásico enrutador de la "vieja escuela", con una buena distribución de los componentes para identificar las diferentes partes del enrutador. Todas las tarjetas madre del enrutador de Cisco utilizan cuatro tipos de memoria, cada una diseñada para llevar a cabo tareas específicas.

Todo enrutador Cisco se envía por lo menos con la cantidad mínima de memoria DRAM y flash. Es posible agregar memoria en la fábrica o actualizarla en el campo. Como regla general, la cantidad de DRAM puede duplicarse o cuadruplicarse (dependiendo del modelo específico) y la cantidad de memoria flash puede duplicarse. Si la densidad de tráfico aumenta con el tiempo, es posible actualizar la DRAM para incrementar la capacidad de utilización del enrutador.

RAM/DRAM

RAM/DRAM son las siglas en inglés de memoria de acceso directo/memoria de acceso directo dinámico. También llamada *almacenamiento de trabajo*, el procesador central del enrutador usa la RAM/DRAM para llevar a cabo su trabajo, de la misma forma que lo hace la memoria en su PC. Cuando un enrutador se encuentra en operación, su RAM/DRAM contiene una imagen del software IOS de Cisco, el archivo de configuración ejecutando, la tabla de enrutamiento, otras tablas (elaboradas por el enrutador después de que se inicia) y el búfer de paquetes.

Que no lo confundan las dos partes en RAM/DRAM. Las siglas sirven para todo. Casi toda la memoria RAM/DRAM de los enrutadores Cisco es DRAM (memoria de acceso directo dinámico). La memoria no dinámica, también denominada *memoria estática*, es obsoleta desde hace varios años, pero el término RAM se usa aún tan ampliamente que se incluye en la literatura para fin de evitar confusión en el tema.

El enrutador más pequeño de Cisco, la Serie SOHO 90, se envía con un máximo de 64 MB de DRAM. En el otro lado del espectro, el enrutador CRS-1, uno de los más grandes de Cisco, soporta hasta 4 GB.

NVRAM

NVRAM son las siglas de RAM no volátil. El término no volátil significa que es memoria que conserva la información después de perder la alimentación de energía eléctrica. Los enrutadores Cisco almacenan una copia del archivo de configuración del enrutador en NVRAM

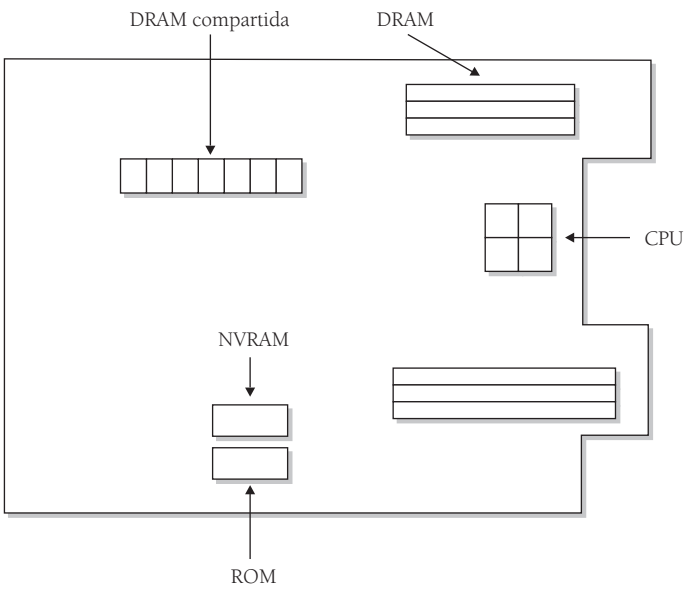


Figura 3-16. Las tarjetas madre de los enrutadores Cisco tienen diseños parecidos.

(más adelante en este capítulo se estudiarán los archivos de configuración). Cuando el enrutador se apaga intencionalmente, o cuando se pierde la alimentación de energía eléctrica, la memoria NVRAM le permite al enrutador reiniciar en la configuración adecuada.

Memoria flash

La memoria flash también es no volátil. Difiere de la NVRAM en que puede borrarse y reprogramarse de acuerdo con lo necesario. Al principio, fue desarrollada por Intel y se utiliza ampliamente en computadoras y otros dispositivos. En los enrutadores Cisco, la memoria flash se utiliza para almacenar una o más copias del software IOS. Ésta es una característica importante, porque permite a los administradores de red utilizar nuevas versiones de IOS en los enrutadores instalados en toda una red y, después, actualizarlos todos de una sola vez con una versión más actual de memoria flash.

ROM

ROM son las siglas en inglés de memoria de sólo lectura. También es no volátil. Los enrutadores Cisco utilizan ROM para almacenar el famoso *programa de arranque*, que es un archivo que se utiliza para iniciar el sistema en un estado de mínima configuración después de una catástrofe. Cuando inicia desde la ROM, lo primero que ve es el indicador rommon>>. ROMMON (de monitor ROM) recuerda a los viejos tiempos del sistema operativo UNIX, que dependían del ROMMON para reiniciar una computadora al punto en que los comandos podían, al menos, ser tecleados en el monitor de la consola del sistema. En los enrutado-

res más pequeños de Cisco, la ROM almacena un subconjunto mínimo del software IOS de Cisco. En algunos enrutadores Cisco, la ROM almacena una copia completa del IOS.

Puertos y módulos del enrutador

Una ventana del enrutador a la red es a través de sus puertos y módulos. Sin ellos, un enrutador no es más que una caja sin uso. Los puertos y módulos que están instalados en un enrutador definen lo que puede hacer.

La interconectividad puede ser intimidante, con una aparentemente infinita cantidad de combinaciones de productos, protocolos, medios de transmisión, características, estándares y demás. Las siglas aparecen de una manera tan rápida y complicada, que parecería un esfuerzo inútil aprender cómo configurar adecuadamente un enrutador. Pero la elección del enrutador correcto puede fragmentarse en partes más manejables. En la tabla 3-4 se despliegan cinco áreas de requisitos principales que, si se logran, lo llevará a obtener la mejor solución para los enrutadores.

Evidentemente, Cisco no puede fabricar un modelo de enrutador que satisfaga las necesidades específicas de cada cliente. Para que su configuración sea más flexible, los enrutadores vienen en dos partes principales:

- ▼ **Chasis** El contenedor real y los componentes básicos dentro de él, como la fuente de poder, los ventiladores, las tapas frontales y traseras, las luces de indicación y las ranuras.
- ▲ **Puertos y módulos** Las tarjetas de circuito impreso que se insertan en el contenedor del enrutador.

La estructura de la línea de productos de enrutadores Cisco lo conducirá a un producto, o al menos a una selección específica de productos, que satisfaga las cinco áreas que se describen en la tabla 3-4.

Área	Descripción	Requisito de configuración
1	Física	El hardware debe ser compatible con el segmento de red físico en que se instalará el enrutador.
2	Comunicación	El enrutador debe ser compatible con el medio de transporte que se utilizará (Frame Relay, ATM, etcétera).
3	Protocolo	Debe ser compatible con los protocolos que se utilizan en la red (IP, IPX, SNA, etcétera).
4	Misión	El enrutador debe proporcionar la velocidad, confiabilidad, seguridad y funcionalidad que requiera la tarea.
5	Negocio	Debe adecuarse al presupuesto y los planes de crecimiento de la red.

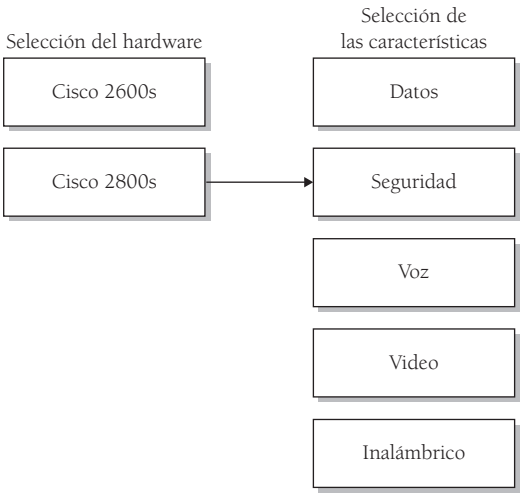
Tabla 3-4. Cinco factores importantes para la selección de un enrutador.

Encontrar el enrutador correcto para sus necesidades es, en esencia, un proceso de tres etapas. A continuación se ilustra el proceso de selección de un enrutador para las operaciones de una sucursal:

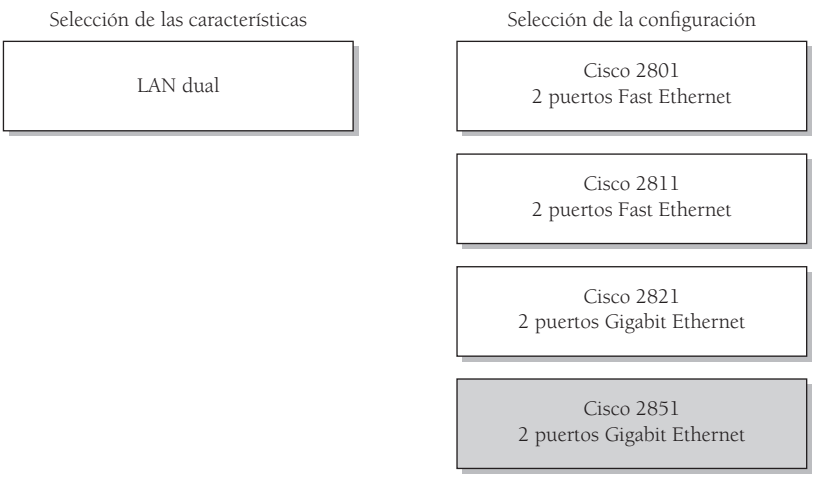
Series de enrutador

Cisco	SOHO	Serie
Cisco	800	Serie
Cisco	1000	Serie
Cisco	2000	Serie
Cisco	3000	Serie
Cisco	7000	Serie
Cisco	10000	Serie
Cisco	12000	Serie

En primer lugar, los enrutadores Cisco se agrupan en familias de productos llamadas *series*. La selección de una serie de productos de enrutador está, en general, determinada por el presupuesto, porque cada serie refleja un tipo de comparación entre precio y desempeño. Los modelos dentro de las series se basan en general en el mismo chasis, que son la estructura metálica y los componentes básicos (fuentes de poder, ventiladores, etcétera) con los que está construido el enrutador. Seleccionaremos la Serie Cisco 2000 porque se ajusta al presupuesto asignado y a las necesidades de desempeño de nuestra sucursal grande.



De la serie 2000, seleccionaremos la serie Cisco 2800. El chasis 2800 es lo suficientemente versátil para ajustarse a un gran número de situaciones, lo que lo convierte en una marca muy popular de enrutadores para sucursales.



En tercer lugar, seleccionaremos el Cisco 2851 porque tiene dos puertos Ethernet; y nuestra sucursal imaginaria trabajará con dos subredes, una para el servicio a clientes y otra para la oficina principal. Los dos puertos Ethernet nos permitirán separar los dos departamentos, aislando con ello el tráfico.

NOTA El término "puerto" puede causar confusión si no se tiene cuidado. Cuando se habla de hardware, un puerto significa una conexión física a través de la cual puede pasar la E/S (por ejemplo, un puerto serial), pero también están los puertos en la capa de transporte de los protocolos de red. Estos "puertos" en realidad son números de puerto que se

utilizan para identificar lo que contiene un paquete de aplicación de la red. A estos puertos (números de puerto) también se les conoce como puertos TCP o UDP o "escuchas", porque informan al receptor lo que hay dentro del mensaje. Como ejemplos de números de puerto definido en TCP están el puerto 25 para el protocolo simple para transferencia de correo (SMTP) y el puerto 80 para HTTP. Consulte la sección del capítulo 2, "La capa de transporte", para conocer más información sobre los puertos TCP y UDP.

Empaquetamiento de un enrutador

Se pueden configurar tres categorías principales de módulos en los enrutadores Cisco para soportar la conectividad LAN o WAN:

- ▼ **Módulos Ethernet** Soportan muchas de las variantes de LAN Ethernet que existen en el mercado, incluidas NetWare de Novell, VINES de Banyan y AppleTalk.
- ■ **Módulos Token Ring** Es la tecnología LAN de IBM, que está bien establecida en bancos, compañías de seguros y otros entornos de corporaciones que aparecen entre las mil más importantes, de acuerdo con la revista *Fortune*.
- ▲ **Módulos de conectividad WAN** Soportan una amplia variedad de protocolos WAN, algunos viejos y otros nuevos. Dentro de los ejemplos de tecnologías WAN se incluyen protocolos más nuevos, como ISDN, Frame Relay, modo de transferencia asincrónica (ATM), además de protocolos antiguos, como el SDLC y X.25.

Las opciones de configuración dependen principalmente del enrutador específico de Cisco:

- ▼ Los enrutadores de extremo inferior tienden a ser de "configuración fija", en el sentido de que los módulos están integrados desde la fábrica (preconfigurados).
- ■ Los enrutadores de alcance intermedio, como la serie 3800 de Cisco, son "modulares" porque aceptan una gran variedad de módulos, a menudo agrupando diferentes protocolos en el mismo contenedor. Los módulos de interfaz se conectan a las tarjetas madre de esta clase de enrutadores.
- ▲ Los enrutadores de extremos superior, como las series 7300 y 12000 de Cisco, cuentan con buses (también denominados *planos posteriores*). Los enrutadores basados en buses aceptan módulos más grandes (en general conocidos como *tarjetas*), que son enrutadores modulares (tienen su propia CPU, unidades de memoria, etcétera).

Modelos de enrutadores Cisco

Cisco ofrece diferentes enrutadores para entornos distintos. Por ejemplo, un ISP no tendrá mucho éxito con un enrutador que sólo pueda acomodar cuatro o cinco usuarios. De la misma forma, no será necesario comprar un enrutador con velocidades del orden de los terabits, de cinco millones de dólares, para una oficina pequeña. A continuación se proporciona una explicación de los diferentes tipos de enrutadores Cisco.

Enrutadores SOHO

SOHO es un término en la industria para usuarios de redes muy pequeñas (oficina pequeña/casera). Los clientes típicos de SOHO cuentan con uno o dos segmentos LAN en sus instalaciones y una conexión ISP a Internet.

Serie de productos	Descripción
Serie 90 de Cisco	Enrutador de acceso DSL para conectar a varios usuarios. Incluye el IOS configurable por el usuario.
Serie 800 de Cisco	Enrutadores ISDN, DSL y de acceso serial para conectar hasta 20 usuarios. Incluye el IOS y tiene la capacidad de codificación VPN.
Serie SB 100 de Cisco	Diseñada específicamente para pequeños negocios, esta serie de enrutadores Ethernet, ISDN y DSL incluye un IOS configurable por el usuario.

Tabla 3-5. Las tres series de enrutadores SOHO de Cisco.

La parte medular de la estrategia SOHO de Cisco son los enrutadores de extremo inferior. Permitir que pequeñas compañías accedan a los ISP de enrutador a enrutador, en lugar de ser usuarios de marcado telefónico, representa un ahorro de dinero en cuanto a conexiones telefónicas, a la vez que mejora la confiabilidad y el rendimiento. En la tabla 3-5 se proporciona un panorama de la serie de productos SOHO de Cisco. El término *serie* se refiere a un chasis que está configurado en varios modelos del producto en la planta de fabricación (lo que suele depender de las tarjetas de circuitos impresos instaladas en ellos).

Los productos SOHO hacen énfasis en las tecnologías de banda ancha (DSL, cable e ISDN), porque las oficinas domésticas y caseras no cuentan con vínculos WAN dedicados, conectados a sus ISP o interconexiones corporativas.

Enrutadores Cisco de rango intermedio

Una red de pequeño o mediano tamaño requiere de una amplia variedad de soluciones. Cisco cuenta con varias capas de acceso a enrutadores diseñados para satisfacer las necesidades de capacidad del cliente y el tipo de vínculo de telecomunicaciones.

Las series que se muestran en la tabla 3-6 representan docenas de números individuales de producto. En función de las series del producto, pueden configurarse diferentes combinaciones de tecnologías LAN y medios WAN. *Modular* significa que el chasis puede actualizarse en el campo insertando uno o más módulos. Los dispositivos no modulares tienen una configuración fija.

Enrutadores de espina dorsal

Cuando Cisco asegura que más de 70% de Internet trabaja con sus enrutadores, éstos son los modelos a los que se refiere. Las series 7000 y 12000 son enormes, con la forma y el tamaño de enormes refrigeradores, y cuentan con buses de datos en que pueden instalarse *tarjetas* (dispositivos completos en una tarjeta).

Serie del producto	Descripción
Serie 1700 de Cisco	Enrutador con acceso a Ethernet para conectarse a un vínculo WAN de banda ancha, ISDN o DSL. Cuenta con codificación VPN y facilidades para VoIP (voz sobre IP) y VoFR (voz sobre Frame Relay).
Serie 1800 de Cisco	Enrutador con acceso a Ethernet para conectarse a ISDN, DSL o banda ancha. Es un enrutador de alta densidad que ofrece soporte a tecnologías 802.11 a/b/g, varias opciones para interfaces WAN y capacidades VPN.
Serie 2600 de Cisco	Es una solución integrada, modular y rentable para trabajo como enrutador de acceso a varios servicios, compuerta de voz/datos o servidor de acceso de marcado telefónico. Conecta una o dos LAN Ethernet o Token Ring a ISDN, T1 canalizado, Ethernet, módems analógicos o enlaces ATM. Además soporta voz, video, FAX y Frame Relay.
Serie 2800 de Cisco	Es un enrutador de acceso modular e integrado. Soporta hasta dos segmentos LAN Ethernet, LAN inalámbrico (802.11 a/b/g), junto con teléfonos IP Cisco.
Serie 3600 de Cisco	Enrutador modular de alta densidad para acceso de marcado telefónico o tráfico de enrutador a enrutador. Soporta ISDN, canales seriales, T1 canalizado, módems digitales y enlaces ATM. Además soporta voz/fax y Frame Relay.
Serie 3700 de Cisco	Una parte fundamental en la tecnología AVVID de Cisco, esta serie de enrutadores de acceso a varios servicios maneja los principales protocolos WAN e incluye dos puertos LAN y tres ranuras WAN.
Serie 3800 de Cisco	Diseñado para sucursales de negocios medianos y grandes, este modelo opera hasta velocidades T3 y es capaz de realizar funciones de datos, seguridad, voz, video e inalámbricas. Esta serie es modular y brinda capacidades de VPN.

Tabla 3-6. Soluciones de enrutamiento de alcance intermedio de Cisco.

Debido a que no son de acceso, los enrutadores de espina dorsal de Cisco pueden tomar todos los usuarios que puedan manejar paquetes. Las siete series de productos (descritas en la tabla 3-7) son modulares, lo que permite que los clientes instalen módulos de acuerdo con la tecnología LAN que se esté ejecutando y la capacidad necesaria. De hecho, estos enrutadores pueden operar más de un protocolo simultáneamente, como Ethernet y Token Ring. Una *ranura* es una bahía electrónica en que se inserta una tarjeta de circuito impreso.

Existe una conexión especializada de alta velocidad utilizada en los enrutadores Cisco de extremo elevado. HSSI son las siglas en inglés de interfaz serial de alta velocidad, un estándar especializado de E/S que se utiliza principalmente en conjunto con supercomputadoras. Los enormes enrutadores 12000 y uBR10012 de Cisco son dispositivos tipo portador, en el sentido de que el equipo local de los operadores de redes de telecomunicaciones los utiliza para sus operaciones de conmutación de datos.

Todos los enrutadores de espina dorsal de Cisco tienen un gran número de facilidades para VPN, seguridad, calidad de servicio (QoS) y administración de la red.

Serie del producto	Descripción
Serie 7200 de Cisco	Tiene cuatro o seis ranuras. Soporta varios protocolos, son escalables y flexibles. Soporta Fast Ethernet, Gigabit Ethernet y paquetes sobre SONET. Proporciona soporte MPLS y velocidades OC-12/STM-4.
Serie 7300 de Cisco	Es un enrutador de una o cuatro ranuras diseñado para una WAN en campus o para proveedores de servicios. Este modelo incluye un firewall, reconocimiento de aplicaciones basadas en red, QoS (calidad de servicio), servicios IP/MPLS y velocidades de datos de hasta OC-48/STM-16.
Serie 7500 de Cisco	Es un enrutador de siete o 13 ranuras que ofrece capacidades de servicios distribuidos y soporta varios protocolos. Esta serie, que presenta alta disponibilidad, incluye conmutación distribuida y una alta densidad de puertos. Proporciona velocidades de datos de hasta OC-12/STM-4.
Serie 7600 de Cisco	Es un enrutador de tres a 13 ranuras con tasa de 240 a 720 Gbps por ranura. Esta serie proporciona un diseño modular y flexible, servicios IP/MPLS y es una mejora de la serie 7500 de Cisco. Proporciona velocidades de hasta OC-48/STM-16.

Tabla 3-7. Series de enrutadores de espina dorsal de Cisco. (*Continúa*.)

Serie del producto	Descripción
Serie 10700 de Cisco	Es un enrutador de dos ranuras que ofrece servicios IP diferenciados a velocidades ópticas de hasta OC-48/STM-16.
Serie 10000 de Cisco	Es un enrutador de conmutación Ethernet Gigabit de ocho ranuras. Tiene una tarjeta especial para vínculos WAN OC-48. Proporciona IPSec y MPLS VPN, además de capacidad para QoS.
Serie 12000 de Cisco	Tiene seis o 15 ranuras y es un enrutador de conmutación Ethernet de 40 Gigabits por ranura para IP. Cuenta con tarjetas especiales para vínculos WAN OC-48 y OC-192.
Serie CRS-1 de Cisco	Tiene de ocho a 16 ranuras y trabaja con el software IOS XR de Cisco, que ofrece un sistema operativo que se repara y protege por sí solo. Soporta tarjetas de líneas modulares y fijas. Es el rey de la línea de enrutadores Cisco y brinda velocidades de terabits con soporte a OC-768.

Tabla 3-7. Series de enrutadores de espina dorsal de Cisco (*conclusión*).

ARCHIVOS ESENCIALES

En contraste con las computadoras normales, los enrutadores Cisco sólo cuentan con dos archivos principales:

- ▼ El archivo de configuración.
- ▲ El software IOS de Cisco.

El software IOS de Cisco contiene instrucciones para el enrutador. El IOS actúa como un agente de tránsito, dirigiendo las actividades dentro del enrutador. El IOS administra las operaciones internas del enrutador, informando a los diferentes componentes de hardware qué hacer, de forma muy parecida a Windows XP o LINUX con una computadora de propósito general. Los clientes no pueden alterar el contenido del archivo IOS.

El archivo de configuración contiene instrucciones para el enrutador introducidas por el cliente, no por Cisco. Contiene información que describe el entorno de la red en que el enrutador funcionará y cómo el administrador de la red desea que se comporte. En pocas palabras, el archivo de configuración le indica *qué* hacer; IOS le indica al enrutador *cómo* hacerlo.

Como se estudiará en el capítulo siguiente, los enrutadores también utilizan archivos dinámicos, que no están almacenados en la memoria flash del enrutador, NVRAM o ROM.

En vez de eso, los archivos dinámicos se construyen desde cero en el momento en que se inicializa un enrutador y son estrictamente reactivos en el sentido de que sólo almacenan información activa y no instrucciones operacionales.

El IOS: el sistema operativo de las interconexiones

Por lo general, no pensamos en un sistema operativo como si fuera un archivo. Después de todo, el sistema operativo de su PC está formado de varios miles de archivos (residen en su directorio con extensiones de archivo como SYS, EXE, DRV y DDL).

Sin embargo, el IOS está, de hecho, contenido en un solo archivo. Cuando envía un archivo IOS a determinado lugar, éste almacena todo lo necesario para hacer funcionar al enrutador. Dependiendo de la versión, una imagen del software del IOS tendrá una capacidad de 3 MB a 10 MB en tamaño.

NOTA Los dispositivos para interconectividad menos sofisticados de Cisco obtienen su inteligencia de un software instalado de fábrica llamado firmware, que es un subconjunto del IOS. Puede actualizarse en el campo para mantener el software del dispositivo actualizado con el resto de la red.

Es necesario que el IOS esté construido de manera muy robusta, porque copias de éste, conocidas como *imágenes del sistema*, se envían rutinariamente entre redes. Las imágenes del sistema se cargan y descargan de los enrutadores con la finalidad de respaldar los enrutadores, actualizar sus capacidades y reinicializarlos después de que se ha presentado una falla. No sería práctico enviar miles de archivos de 50 MB. La posibilidad de enviar un solo archivo IOS pequeño hace posible la administración efectiva de la red.

Conjuntos de características del IOS

Los *conjuntos de características* son paquetes que tratan de simplificar la configuración y el orden del software IOS. No se da soporte, en sí, a ningún producto de software del IOS. En realidad, IOS es una plataforma común de software que sirve como base por una arquitectura de implementaciones del IOS, cada una de las cuales está empaquetada para cumplir con una misión específica. Cisco llama a estos paquetes IOS *conjuntos de características* (también denominados *imágenes de software* o *paquetes de características*). Cuando ordena un enrutador Cisco, selecciona un conjunto de características de IOS que contiene todas las capacidades que requiera su situación en particular. Casi todos los requisitos se relacionan con el mantenimiento de la compatibilidad con los diferentes dispositivos de hardware y protocolos de red en los entornos en que trabajará el enrutador.

Como se muestra en la figura 3-17, las variantes del software IOS de Cisco se definen de dos maneras: por conjunto de características y por versión. Los conjuntos de características definen las tareas que una versión del IOS puede realizar; las versiones se utilizan para administrar el software IOS con el tiempo.

Los conjuntos de características del IOS de Cisco están diseñados para:

- Ser compatibles con ciertas plataformas de enrutadores.
- Permitir la operación entre protocolos de conectividad diferentes (NetWare de Novell, SNA de IBM, AppleTalk, etcétera).

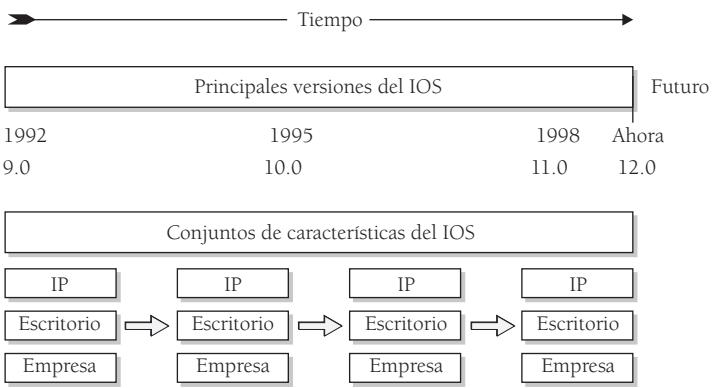


Figura 3-17. El IOS está organizado por versiones y conjuntos de características.

- ▲ Proporcionar características funcionales en la forma de servicios y aplicaciones de red para aspectos como administración de red, seguridad y multimedia.

El empaquetamiento y la venta de software del IOS de esta manera simplifican las cosas para Cisco y los clientes. Para el cliente, contar con un solo número de parte simplifica la operación de seleccionar qué software comprar. En el caso de Cisco, ayuda a los ingenieros de producto de la compañía a tener una idea de dónde va cada elemento, de modo que su personal de soporte sepa quién tiene cada cosa. Recuerde que la interconectividad puede volverse irremediablemente compleja porque la naturaleza del negocio es permitir que plataformas de cómputo y protocolos de conectividad diferentes operen entre sí y puedan coexistir.

Cómo están construidos los conjuntos de características Debido a que los conjuntos de características dependen del hardware del enrutador en que trabajan, se aplican dos reglas:

- ▼ No puede ejecutar todos los conjuntos de características en todas las plataformas del enrutador.
- ▲ A veces, las características específicas dentro de un conjunto se ejecutarán o no en función de la plataforma del enrutador.

Si echa un vistazo al catálogo de productos de Cisco, le costará trabajo comprender el conjunto de características a primera vista. Los conjuntos de características no hacen otra cosa que colocar agrupaciones funcionales en paquetes lógicos que los clientes puedan utilizar. De una manera u otra, todos los conjuntos de características derivan su funcionalidad de una docena de categorías, que se muestran en la tabla 3-8.

No se preocupe por los ejemplos que se muestran en el lado derecho de la tabla o todas las siglas que no conozca. Lo importante es que comprenda que el software IOS contiene características y funciones que pueden agruparse en una docena de categorías.

Los conjuntos de características del IOS de Cisco tratan de combinar éstas en grupos que satisfagan casi todas las necesidades reales de los clientes. Cisco proporciona docenas

de conjuntos de características de productos en forma de números de productos de software del IOS que pueda colocar en una orden de compra. Están agrupados por características generales en las cuatro familias que se muestran en la tabla 3-9. En las tablas 3-8 y 3-9 se observa que las plataformas de cómputo de propietario, como IBM, DEC y Apple y plataformas de redes de propietario, como Novell y SNA, orientan en gran medida la necesidad de conjuntos de características. Cada enrutador de Cisco debe atender las necesidades reales de compatibilidad del cliente, lo que significa tener la capacidad de operar con hardware y software heredados. Casi todas las arquitecturas tradicionales existen en la "orilla de la red" (lo que significa que casi todo el equipo de propietario con el que IP debe mantener compatibilidad reside en las LAN o en las computadoras que residen en las LAN). Aquí es donde se manifiestan los problemas de compatibilidad con arquitecturas heredadas de propietario o con plataformas especializadas.

Categoría	Ejemplos de características
Soporte LAN	IP, IPX de Novell, AppleTalk, Banyan VINES, DECnet.
Servicios WAN	PPP, emulación LAN de ATM, Frame Relay, ISDN, X.25.
Optimización de las WAN	Marcado telefónico por demanda, enrutamiento rápido, planeación del tráfico.
Enrutamiento IP	BGP, RIP, IGRP, IGRP Mejorado, OSPF, IS-IS, NAT.
Otro enrutamiento	RIP de IPX, AURP, NLSP.
Multimedia y QoS	Planeación del tráfico genérico, detección aleatoria temprana, RSVP.
Administración	SNMP, RMON, Call History MIB de Cisco, Perfiles Virtuales.
Seguridad	Listas de acceso, listas de acceso extendido, cerrar con llave, TACACS+.
Conmutación	Enrutamiento con política de conmutación rápida, Enrutamiento AppleTalk sobre ISL.
Soporte de IBM	APPN, Bisync, Frame Relay para SNA, integración SDLC.
Traducción de protocolos	LAT, PPP, X.25.
Nodo remoto	PPP, SLIP, MacIP, fondo IP, CSLIP, NetBEUI sobre PPP.
Servicios terminales	LAT, Xremote, Telnet, X.25 PAD.

Tabla 3-8. Categorías de las características del software del IOS.

En las tablas 3-8 y 3-9 también se muestra cuáles agrupaciones funcionales de software van con cada producto de IOS. Por ejemplo, es muy probable que las compañías multinacionales estén interesadas en la funcionalidad de IBM, como NetBEUI sobre PPP y Frame Relay para SNA, y tal vez estén interesadas en uno de los grupos de características Empresa y APPN. En contraste, una agencia de publicidad que tenga mucho equipo de Apple y Windows se concentrará en los conjuntos de características de escritorio.

La agrupación de conjuntos de características en familias representa la forma en que Cisco mantiene cierto orden en las políticas de precios y las rutas de actualización. Ordenar un solo número de parte IOS en lugar de docenas ayuda a todos a evitar errores. En la figura 3-18 se muestra el proceso de la selección de los conjuntos de características.

Conjunto de características	Entorno objetivo del cliente
Base IP	Enrutamiento IP básico.
Voz IP	Enrutamiento de voz IP.
Base empresarial	Funcionalidad de extremo alto para LAN, WAN y la administración.
Seguridad avanzada	Características avanzadas de seguridad.
Servicios empresariales	Incluye las características de la base empresarial, junto con los servicios de voz, ATM y soporte MPLS.
Servicios IP avanzados	Incluye la funcionalidad de Base y Voz IP, junto con ATM, MPLS y soporte de seguridad.
Servicios empresariales avanzados	Lo mismo que empresarial pero con características adicionales de seguridad.

Tabla 3-9. Familias de conjuntos de características de IOS.

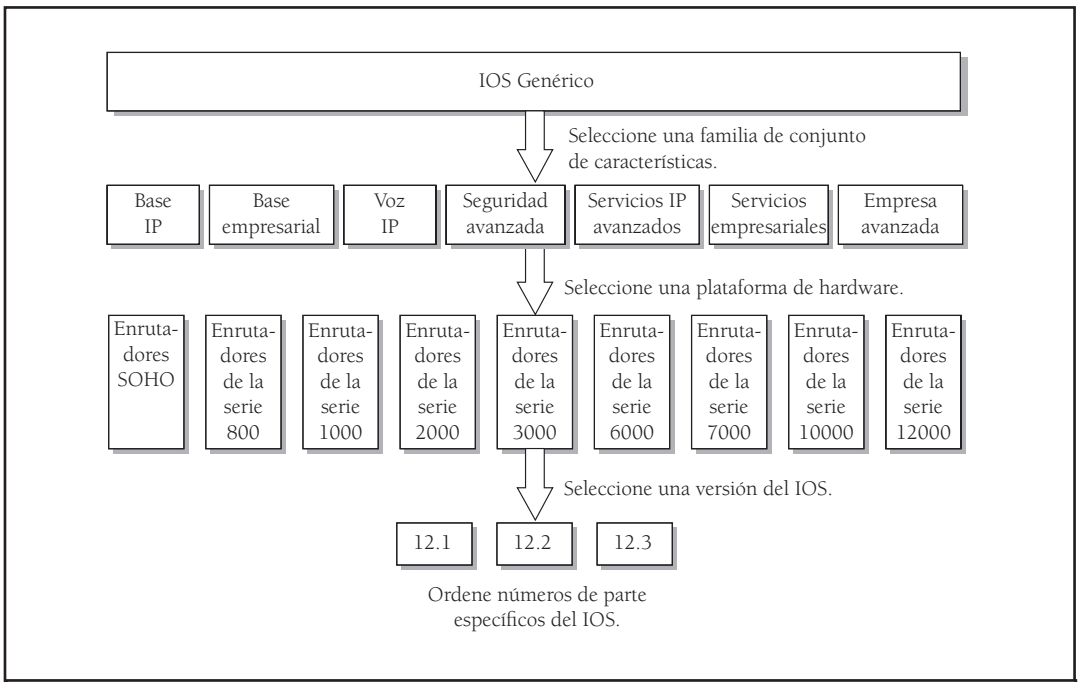


Figura 3-18. El proceso de configuración de un conjunto de características específicas del IOS incluye la selección de los atributos deseados.

Por último, los conjuntos de características se agrupan en variantes de productos de software:

- ▼ **Básicos** El conjunto de características básicas para la plataforma de hardware
- ■ **Plus** El conjunto de características básicas y adicionales que dependen de la plataforma seleccionada.
- ▲ **Cifrado** La adición de una característica de cifrado de 40 bits (Plus 40) o 56 bits (Plus 56) arriba del conjunto de características Básico o Plus.

El objetivo final de los conjuntos de características es guiarlo por el proceso de colocar una orden, digamos, el conjunto de características del IOS Empresarial 56 para un 7500/RSP de Cisco que ejecuta la versión 11, sin cometer un error que pueda costarle al proyecto de actualización de su red un retraso de dos semanas.

La anatomía de los números de versión de Cisco Los números de versión del software IOS de Cisco tienen cuatro partes básicas, como se muestra en la figura 3-19.

La primera parte es el versión principal (el "12" en la figura 3-19), que marca los primeros envíos al cliente (FCS), de una versión IOS de software estable de alta calidad para que los clientes lo utilicen en sus redes de producción. Las versiones principales se dividen de la siguiente manera:

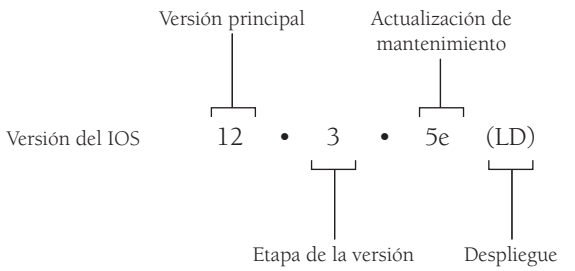


Figura 3-19. Existen cuatro partes primordiales en un número de versión del IOS.

- **Etapa** El "3" en la figura 3-19, que marca el FCS de varias etapas principales de la versión (la primera versión, la versión de uso general, la versión de corta vida, etcétera) A menudo se hace referencia a las etapas de versiones en tiempo futuro, cuando están planeadas pero no se han lanzado.
- **Actualización de mantenimiento** El "5e" de la figura 3-19, denota el soporte para plataformas adicionales de características, más allá de lo que estaba disponible en la versión principal del FCS.

La cuarta parte del número de versión es el despliegue. Una versión de despliegue general (GD) es para un uso sin restricciones por parte de todos los usuarios. Los versiones de despliegue temprano (ED) entregan nuevas funcionalidades y tecnologías a los clientes para desplegarse en forma limitada en sus redes. El despliegue limitado (LD) denota un ciclo de vida limitado entre el FCS y el GD.

En cualquier momento, puede haber varias versiones importantes en uso en el campo. Por ejemplo, están disponibles cinco versiones del IOS 12, pero la 11.2 y la 11.3 aún están en uso. La mayoría de los administradores de redes se sienten a gusto aferrándose a un versión que saben que les va a funcionar. Otros utilizan versiones avanzadas de IOS en etapas temprana porque necesitan obtener soporte que no se encontraba disponible para la plataforma o la característica. La mayoría de los usuarios están felices que los usuarios más antiguos ayuden a Cisco a arreglar las cosas antes de la versión general.

NOTA En este libro, utilizamos el término "versión" para especificar un versión determinada de un conjunto de características de IOS en particular.

Empleo del TFTP para realizar actualizaciones y respaldos del IOS

En el caso de una catástrofe en la red, es posible que la imagen del sistema IOS del enrutador sea destruida o borrada de la memoria flash. El procedimiento estándar consiste en mantener una imagen de respaldo de cada versión del IOS en uso en la red que se está administrando. Estas imágenes IOS de respaldo se mantienen en los servidores TFTP o dentro de las aplicaciones de administración de la red, como CiscoWorks (que se estudia en el capítulo 13).

TFTP son las siglas en inglés de protocolo trivial de transferencia de archivos. TFTP es una aplicación TCP/IP derivada de los primeros días del sistema operativo UNIX. Como adivinará, TFTP es una versión más burda de FTP, el comando que muchos utilizan para descargar archivos de Internet. El IOS utiliza TFTP en lugar de FTP, porque es más veloz y utiliza un menor número de recursos del sistema.

Los llamados servidores TFTP son plataformas de computadoras en una interconexión que almacenan y descargan imágenes del sistema IOS y archivos de configuración. Se recomienda que se utilice más de un servidor TFTP para respaldar una red. Esto es en caso de que el servidor TFTP falle o que el segmento de red que lo conecta a los dispositivos que respalda no esté disponible.

Para cargar una imagen nueva del IOS a una memoria flash del enrutador, utilice el comando **copy tftp flash** siguiendo el procedimiento que se muestra enseguida:

```
Router#copy tftp flash

System flash directory:
File  Length   Name/status
  1   4171336  c4500-j-mz_112-15a.bin
[4171400 bytes used, 22904 available, 4194304 total]
Address or name of remote host [10.1.10.40]? 10.1.10.40
Source file name? c4500-j-mz_112-15a.bin
Destination file name [c4500-j-mz_112-15a.bin]? <cr>
Accessing file ‘c4500-j-mz_112-15a.bin’ on 10.1.10.40...
Loading c4500-j-mz_112-15a.bin from 10.1.1.12 (via TokenRing1): [OK]

Erase flash device before writing? [confirm]yes
Flash contains files. Are you sure you want to erase? [confirm]yes

Copy ‘c4500-j-mz_112-15a.bin’ from server
  as ‘c4500-j-mz_112-15a.bin’ into Flash WITH erase? [yes/no]yes
Erasing device... eeeeeeeeeeeeeeee ...erased
Loading c4500-j-mz_112-15a.bin from 10.1.1.12 (via TokenRing1): !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4171336/4194304 bytes]

Verifying checksum...  OK (0x29D5)
Flash copy took 00:00:30 [hh:mm:ss]
Router#
```

Verá que el servidor TFTP confirmó que tenía la imagen del sistema IOS antes de sobrescribir el de la memoria flash del enrutador. Cada signo de admiración en la pantalla indica que un bloque del archivo se copió con éxito en la red del servidor al enrutador.

NOTA Si está copiando un archivo a un servidor TFTP, asegúrese de que el nombre del archivo que está tratando de transferir ya exista en el directorio TFTP. Cree el archivo en los sistemas UNIX utilizando el comando **touch**. En las plataformas de Microsoft, abra el bloc de notas para crear el archivo y guárdelo bajo el nombre del archivo.

El archivo de configuración

La administración de un enrutador incluye la instalación, la actualización, el respaldo, la recuperación y otras tareas dependientes de los eventos, pero la parte más importante de la administración del enrutador es el cuidado y la alimentación de datos de un archivo de configuración del enrutador. El archivo de configuración es el punto de control desde el cual el administrador de la red opera el enrutador y todo el tráfico que pasa por él. Como se detallará en el capítulo siguiente, los archivos de configuración contienen listas de acceso, contraseñas y otras herramientas importantes para la administración del enrutador.

Visualización del archivo de configuración

La forma más común de examinar el *status* de un enrutador consiste en ver su archivo de configuración. Para ver casi todo lo que hay en el IOS, se debe solicitar la vista de la configuración. El comando principal del IOS para ver dicha información es el comando **show**.

El ejemplo siguiente utiliza el comando **show running-config** para ver la configuración de ejecución de un enrutador. Existen dos tipos de archivos de configuración. El *running* es una imagen que funciona en la DRAM (memoria principal) en un momento dado. El *backup* se almacena en la NVRAM y se utiliza para arrancar el enrutador.

```
Router#show running-config
Building configuration...
Current configuration:
!
version 12
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$C/q2$ZhtujqzQIuJrRGqFwdwn71
enable password 7 0012000F
!
vty-async
!
interface Serial0
 no ip address
```

```
 no ip route-cache
 no ip mroute-cache
 shutdown
! interface Serial1
 no ip address
.
.
.
```

En el siguiente capítulo, estudiaremos con más detalle lo que hace el archivo de configuración y cómo editarlo.

El uso del TFTP para actualizaciones y copias de seguridad del archivo de configuración

De la misma forma que con las actualizaciones y copias de seguridad de la imagen del sistema IOS, el TFTP se utiliza para respaldar y actualizar los archivos de configuración. Por ejemplo, el comando **copy running-config tftp** se utiliza para crear una copia de seguridad del archivo de configuración que funciona en el enrutador (llamado tomtest en este ejemplo) en un servidor TFTP, utilizando el procedimiento siguiente:

```
Router#copy running-config tftp
Remote host []? 10.1.10.40
Name of configuration file to write [router-config]? test
Write file tomtest on host 10.1.10.40? [confirm]<cr>
Building configuration...

Writing test !! [OK]
Router#
```

Los otros comandos TFTP para crear copias de seguridad y actualizar los archivos de configuración son:

- ▼ **copy tftp running-config** Configura el enrutador directamente al copiar del TFTP directamente a la DRAM del enrutador.
- ■ **copy startup-config tftp** Respalda la configuración de arranque desde la NVRAM del enrutador al servidor TFTP.
- ▲ **copy tftp startup-config** Actualiza el archivo de configuración de arranque del enrutador, descargándolo del servidor TFTP y sobrescribiendo el que se almacenó en la NVRAM del enrutador.

Observe que **tftp** va *frente al* tipo de archivo (**running-config** o **startup-config)** para descargar (actualizar desde el servidor) y *detrás* del tipo de archivo para cargar (crear una copia de seguridad en el servidor). Imagine que el comando **copy** es como si copiara *de* algún lugar *a* otro lugar.

CAPÍTULO 4

Configuración de enrutadores

El enrutador es la parte medular de la interconectividad. Es el dispositivo que entrelaza las redes en interconexiones y las hace útiles. Así que si aprende cómo administrar adecuadamente los enrutadores, es posible que pueda administrar una interconexión. El único punto de control sobre el enrutador con el que cuenta el administrador de redes es el archivo de configuración, también llamado *config file* o archivo config, para abreviar. El archivo de configuración es uno de los dos archivos permanentes de un enrutador. El otro es el software IOS, que es de naturaleza general y no puede ser modificado por los clientes. El archivo de configuración es, entonces, el único punto de control sobre la red con el que cuenta el administrador y se encuentra en la parte medular de las operaciones del enrutador. El IOS hace referencia a dicho archivo cientos de veces por segundo con la finalidad de informarle al enrutador cómo hacer su trabajo.

A pesar de que el archivo de configuración es una herramienta clave, puede parecer difícil de comprender al principio. Lo anterior se debe a que es diferente a los tipos de archivos al que la mayoría de nosotros estamos acostumbrados. No puede colocar un cursor en uno de ellos y editarlo en tiempo real como lo haría, digamos, con un documento de un procesador de palabra. No puede compilarlo y depurarlo de la misma forma en que los programadores convierten el código fuente en ejecutable. Los archivos de configuración se modifican ingresando comandos IOS y, después, observando la nueva configuración para ver si se ha llegado al resultado deseado.

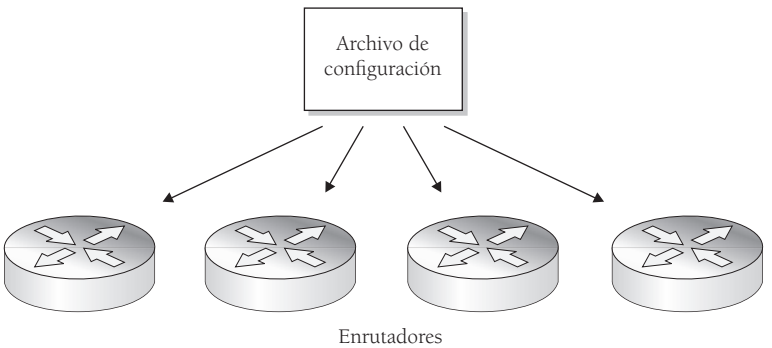
EL PAPEL PRIMORDIAL DEL ARCHIVO DE CONFIGURACIÓN

La mayoría de los problemas de red son causados por problemas de configuración y no por fallas en el hardware o por errores en los circuitos de telecomunicaciones. Si lo piensa detenidamente, esto no es sorprendente. Al archivo de configuración es adonde va toda la información de los administradores de red y, por tanto, donde es más probable que se manifieste un error humano. Como se estudió en el capítulo anterior, un enrutador, en sí, es un dispositivo complejo. Coloque uno en una interconexión (donde el enrutador interactúa con otros) y comprenderá cómo está saturado de interdependencias el archivo de configuración de un enrutador promedio. Cada enrutador que se agregue a una interconexión incrementa la complejidad de manera exponencial. De esto se deduce que cada vez que haga un cambio en el archivo de configuración, la complejidad se convertirá en algo más difícil de identificar.

Los errores de configuración no necesariamente se manifiestan de inmediato como problemas de operación. Muchos problemas son difíciles de ver (y, por tanto, difíciles de evitar), porque permanecen latentes (en los archivos de configuración de la red, esperando hacerse presentes en el momento menos pensado).

Así que cuando la gente de interconexiones habla de "configurar" un enrutador, no habla de poner algunos componentes en el gabinete, sino de hacer cambios en el comportamiento del enrutador y considerar todo lo que se presente a partir de esos cambios. Por naturaleza, las interconexiones tienden a magnificar las cosas transfiriéndolas por la línea. Ésta es la razón por la que los administradores de red dedican todo su esfuerzo de diseño y planeación a lo que parecería algo sin consecuencias serias para un novato. Los administradores de red invierten una gran cantidad de su tiempo cambiando y revisando los archivos de configuración, porque ahí es donde se define todo.

Para magnificar aún más la importancia del diseño del archivo de configuración, encontramos el hecho de que el archivo de configuración promedio incorpora muchos de los estándares especificados por la empresa. Éstos, en general, se aplican a más de un enrutador. Definitivamente, la administración de la red no se lleva a cabo de enrutador en enrutador. En general, los archivos de configuración se mantienen en grupos de enrutadores en masa, tomando en cuenta los parámetros específicos del enrutador. Por ejemplo, los vínculos y las direcciones IP difieren de uno a otro. La distribución en masa de los archivos de configuración se hace tanto por control de diseño como por conveniencia. Es una forma de asegurar la consistencia de que las interconexiones necesitan operar sin problemas.

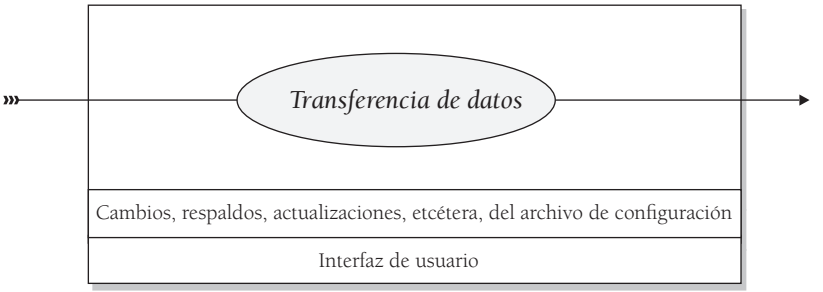


Los diseñadores de redes suelen dividir los grupos de enrutadores en subgrupos (o clases) con características comunes que tienen que ver con áreas de red, versiones de software del equipo y necesidades de seguridad. Por tanto, tiene sentido implementar modificaciones, mejoras, pruebas, etcétera, en las políticas de la red *en masa* para las cargas y descargas del archivo de configuración. Éste sólo se trata de manera individual cuando se presenta un problema con una máquina en particular.

Tres tipos de archivos de enrutadores Cisco

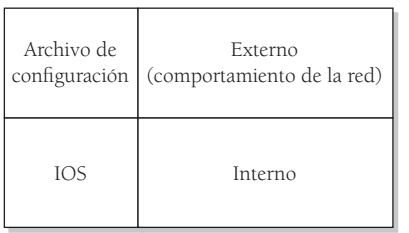
Se utilizan tres tipos de archivos para poner a funcionar un enrutador Cisco: los dos archivos permanentes (la imagen IOS y el archivo de configuración) y los archivos creados y mantenidos por el propio enrutador. Es importante contar con una idea acerca de cómo trabajan en conjunto dichos archivos.

Como con cualquier sistema operativo, la función del IOS es hacer funcionar la computadora en que reside. Difiere con respecto a otros sistemas operativos en que su objetivo primordial es transferir paquetes hacia dentro y fuera del gabinete. Mientras que otros sistemas operativos se encargan de la interacción con los usuarios, el manejo de los números, la salida de impresión y cosas por el estilo, el IOS sólo se encarga de transferir los paquetes que no han sido modificados, hacia su destino siguiente. Sólo se encarga de proporcionar soporte a una interfaz de usuario, en la medida en que es necesaria, para que los administradores de la red se encarguen de llevar a cabo otras tareas internas.

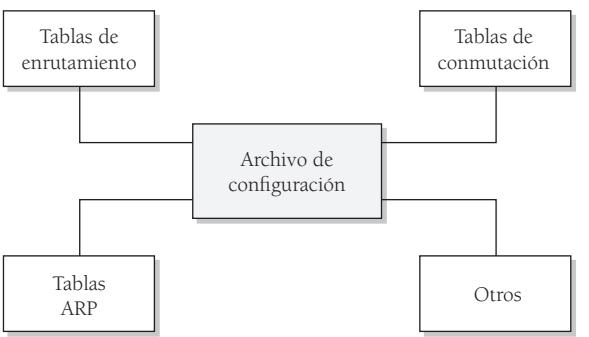


Prioridades de las operaciones del IOS

El archivo de configuración es donde se colocan las instrucciones de administración con el fin de informar al IOS cómo funcionar adecuadamente en la interconexión. El archivo de configuración define el hardware de la interfaz de la red que está en el gabinete del enrutador, los protocolos soportados, cuáles paquetes pueden pasar, etcétera. En pocas palabras, el archivo de configuración es donde los administradores de red almacenan todo su trabajo. Una vez que haya aprendido a trabajar bien utilizando los archivos de configuración, habrá obtenido un dominio de los fundamentos de la administración de la interconexión.



Pero el enrutador genera varios archivos propios. Estos archivos (a menudo llamados *archivos dinámicos*) sólo salen a escena después de que se enciende el enrutador. Si lo apaga, los archivos dinámicos "desaparecen" (sólo la imagen IOS y el archivo de configuración se almacenan permanentemente).



El enrutador crea y mantiene archivos dinámicos para adaptarse minuto a minuto, razón por la cual no sería práctico que una persona los mantuviera actualizados. Sin embargo, a pesar de que los administradores de red no pueden escribir instrucciones en los archivos

dinámicos, sí pueden controlar indirectamente el comportamiento de los archivos dinámicos estableciendo parámetros en el archivo de configuración. Asimismo, con mucha frecuencia los administradores examinan el contenido del archivo dinámico para reparar las fallas que se presentan en la red. Los detalles del funcionamiento de los diferentes archivos dinámicos se estudiarán en capítulos posteriores. Por ahora, sólo recuerde lo siguiente:

- ▼ No puede colocar información directamente en los archivos dinámicos.
- ■ El contenido de los archivos dinámicos cambia minuto a minuto, como respuesta a las tendencias del tráfico de la red (por eso se les llama "dinámicos").
- ▲ El control sobre los archivos dinámicos es indirecto, mediante los parámetros establecidos en el archivo de configuración.

IOS	Archivo de configuración	Archivos dinámicos.
Versiones, conjuntos de características.	Instrucciones de operación.	Información temporal.

Considerados en conjunto, el IOS, el archivo de configuración y los archivos dinámicos conforman el entorno operacional del enrutador. El archivo de configuración es el punto de control medular sobre los enrutadores y, por tanto, sobre todas las redes. El IOS se deja a los ingenieros de software de Cisco; usted lo controla solamente cargando nuevas versiones aproximadamente cada año. Los archivos dinámicos se controlan indirectamente. Por tanto, todos los cambios de administración de las redes están incluidos en el archivo de configuración.

Dado que no puede editar los archivos de configuración en forma interactiva, el proceso de administrar los enrutadores Cisco tiende a ser más indirecto que lo que la mayoría de nosotros estamos acostumbrados. En la figura 4-1 se muestra el proceso típico de modificación del archivo de configuración.

Para algunos, la combinación de una interfaz de usuario basada en caracteres y del proceso indirecto de administración inherente a los enrutadores, parece complicada. Pero la interconectividad es más fácil de lo que aparenta. La comprensión de estos hechos sencillos ayudará al principiante a iniciarse en el análisis y la reparación de problemas de la red:

- ▼ El IOS es su interfaz; usted utiliza los comandos IOS para interactuar con el enrutador.

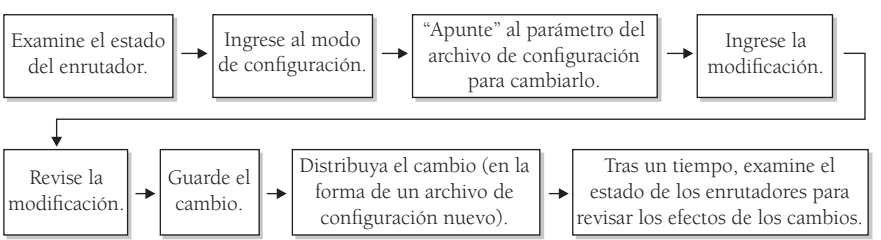


Figura 4-1. La administración de los archivos de configuración incluye muchos pasos.

- El archivo de configuración y los diferentes archivos dinámicos almacenan la información que usted necesita para analizar los problemas de la red.
- El archivo de configuración le dice cómo está configurado un enrutador; los archivos dinámicos muestran cómo está trabajando la configuración en el entorno de red.
- El archivo de configuración es su único punto de control.
- ▲ No puede editar directamente el archivo de configuración; tiene que modificarlo por medio de los comandos del IOS y, después, revisar los resultados.

Ahora que sabe cómo trabajar con un enrutador, es hora de que adquiera experiencia práctica. Si tiene acceso a un enrutador Cisco, ingrese al sistema y siga las instrucciones.

COMIENCE A TRABAJAR CON LOS ENRUTADORES CISCO

Para configurar y administrar enrutadores Cisco, es necesario que sea capaz de interactuar con ellos por medio de algún tipo de conexión. En primera instancia, debe comunicarse de alguna forma con el enrutador, ya sea accediendo o bajando y subiendo archivos a él. Una vez que se ha conectado con éxito a un enrutador, debe hablar su idioma, que en el caso de los enrutadores Cisco son los comandos del IOS.

Comunicación con el IOS

Puede acceder a un enrutador directamente a través del puerto de la consola y el AUX, o mediante una red que utilice los protocolos Telnet, SSH (Secure Shell), HTTP o HTTPS. Los profesionales en redes suelen utilizar SSH por conveniencia y seguridad. Tenga presente que una vez que se establece una sesión, Telnet y SSH son esencialmente lo mismo, excepto por una característica importante (el tráfico SSH será totalmente codificado mientras que el de Telnet no). Cualquiera que sea el método que se utilice, necesita acceder al ambiente IOS para revisar los archivos e ingresar comandos. Los clientes Telnet y SSH suelen estar disponibles en todos los sistemas operativos. Un cliente muy popular es PuTTY, que se encuentra disponible en www.putty.nl. Una vez que lo haya descargado de la red, lo único que necesita para iniciarlo es un doble clic en él.

Como se observa en la figura 4-2, se pueden acceder a los anfitriones remotos o locales. La dirección IP que se resalta en la figura 4-2 es para un enrutador conectado a la red de área local (LAN) en la misma oficina que nuestro administrador de red imaginario. Se utilizaría una de las direcciones IP remotas si el enrutador estuviera localizado en un sitio remoto (esto es, más allá de la LAN). Aunque esté en la misma red que el enrutador, se debe ingresar una contraseña válida para obtener acceso.

Sólo por si acaso algún día se la encuentra, en la figura 4-3 se muestra una condición de error que suele aturdir a los principiantes cuando ingresan sus primeros comandos del IOS.

Lo que está pasando en la figura 4-3 es esto: cuando ingresa texto que el IOS no puede interpretar como comandos, supone que es un nombre simbólico para una dirección IP. El IOS no puede elegir a este respecto. Después de todo, uno de los propósitos del enrutador es comunicarse con otros enrutadores y no hay un solo enrutador que tenga en un archivo todas las direcciones existentes. Aquí, el enrutador intenta enviar el nombre de la dirección

simbólica a todas las direcciones dentro de su dominio. Las transmisiones tienen siempre la dirección 255.255.255.255 (como recordará del capítulo 2). Después de casi diez segundos, el enrutador dejará de hacer envíos, desplegará un mensaje de error y regresará al indicador de comandos.

NOTA En casi todos los sistemas operativos, si ingresa un comando erróneo, obtendrá un mensaje de error. Si usted proporciona un comando erróneo al IOS, éste supondrá que lo que ingresó es una dirección de red y tratará de usar Telnet. Los sistemas operativos normales conocen todos los posibles valores de entrada que pueden ir en ellos, pero IOS no se puede dar ese lujo. Éste trabaja con direcciones de red, y los enrutadores nunca suponen que conocen todas las direcciones posibles porque las redes cambian constantemente.

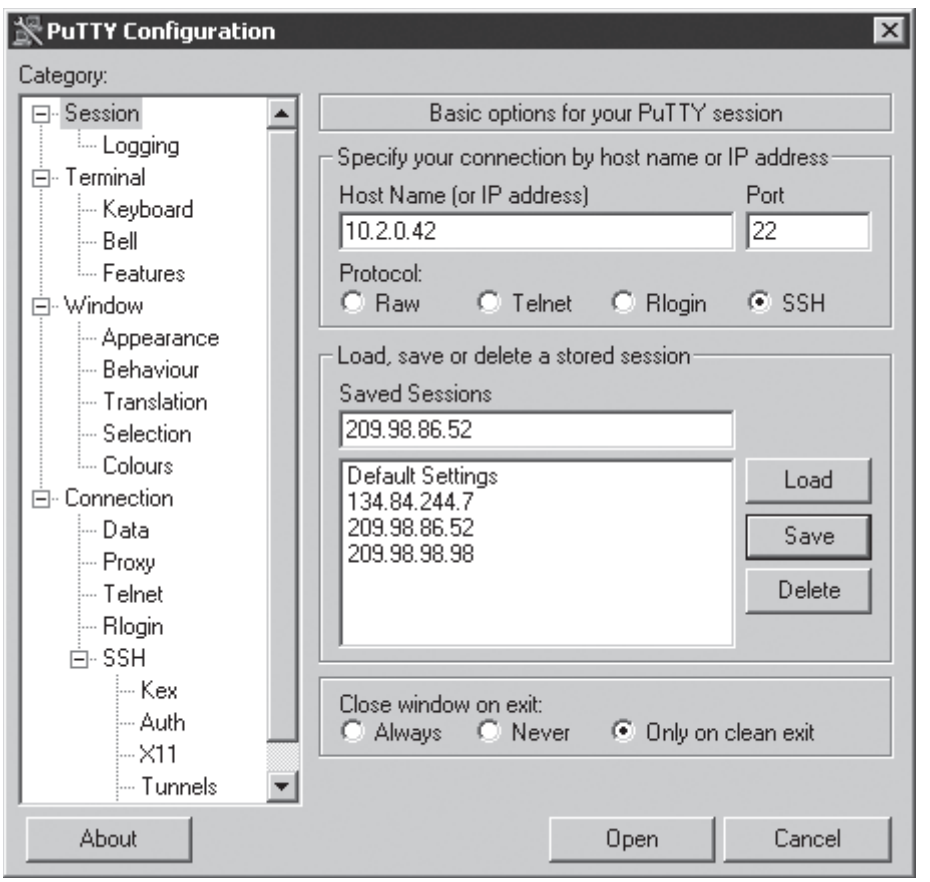


Figura 4-2. La configuración se realiza al iniciar sesión en un enrutador mediante una conexión Telnet.

```
mail.ccie4u.com - PuTTY

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2610XM (MPC860P) processor (revision 0x100) with 94208K/4096K bytes of mem
ory.
Processor board ID JAE072911NU (537772905)
M860 processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2142

Router>ThisIsMyBadCommand
Translating "ThisIsMyBadCommand"...domain server (255.255.255.255)

Translating "ThisIsMyBadCommand"...domain server (255.255.255.255)
 (255.255.255.255)% Unknown command or computer name, or unable to find computer
 address
Router>
```

Figura 4-3. El ingreso de un comando erróneo genera un mensaje de transmisión inadvertida.

Conozca el IOS 12.4

IOS versión 12.4 cuenta con gran cantidad de mejoras sobre las plataforma IOS anteriores. Existen cientos de nuevas características en el IOS, mucho más que el espacio con el que se cuenta aquí para estudiarlas. Una vez dicho esto, echemos un vistazo a algunos de los cambios significativos del IOS versión 12.4.

Al igual que con cualquier sistema operativo nuevo, no es inteligente (y ni siquiera necesario) realizar inmediatamente el cambio a uno nuevo sin comprender primero el impacto que puede tener en su red. Cisco recomienda actualizarse a la versión 12.4 a los clientes que están utilizando la versión 12.3T, puesto que el 12.4 proporciona mantenimiento para esa versión, una vez que ésta llega a su etapa final de ingeniería. Sin embargo, más allá de esto, es una buena idea considerar lo que está utilizando y determinar si las nuevas características de la versión 12.4 valen la pena para usted.

Soporte del hardware

Cisco ha saturado la lista del hardware que soporta el IOS 12.4. Éste incluye los Network Analysis Modules (NAM, módulos para el análisis de la red) para los enrutadores modulares, los enrutadores ISP, Cisco Unity Express y el módulo de red IDS.

Banda ancha

La banda ancha incluye la agregación DSL, las características MPLS y las características de marcación telefónica. La banda ancha es sin duda la tecnología que más ha prevalecido (y, desde luego, la más útil), pero algunas de estas características pueden ser un poco más especializadas de las que el usuario de IOS promedio necesitará implementar.

Gran disponibilidad

IOS versión 12.4 brinda una disponibilidad mejorada a través de dos características:

- ▼ **Actualización en línea** El IOS se descomprime y carga en la memoria, haciendo más fácil el proceso. La nueva imagen no necesita cargarse en la memoria rápida para hacer esto.
- ▲ **Recuperación de fallas basada en estado de IPSec del IOS de Cisco** Permite que un enrutador siga procesando y enviando paquetes IPSec después de una falla de energía.

Infraestructura

La infraestructura se mejoró en dos áreas:

- ▼ **Administrador de eventos IOS de Cisco versión 2.1** Detecta eventos y dispara acciones en la línea de comandos local dentro de un enrutador.
- ▲ **Administrador de recursos insertados** Permite el monitoreo de los recursos internos y el desempeño de acciones con el fin de mejorar el desempeño y la disponibilidad del enrutador.

Movilidad IP

La movilidad IP se mejora mediante las mejoras a NAT y Dynamic Security Associations and Key Distribution.

Transmisión múltiple de IP

Entre las mejoras a la transmisión múltiple de IP se incluyen:

- ▼ Nuevas características de transmisión múltiple IPv6.
- ■ Mejoras al Multicast Source Discovery Protocol (MSDP, protocolo de descubrimiento de fuente de transmisión múltiple).
- ▲ PIM-Dense Mode (PIM-DM) Fallback Prevention (prevención de retroceso del modo denso PIM, PIM-DM). Lo anterior permite que se evite el PIM-DM en situaciones de transmisión múltiple.

Enrutamiento IP

Seguramente esperaría que el enrutamiento IP tuviera gran cantidad de cosas nuevas, pero en realidad no las tiene. De todos modos, no hay mucho de qué preocuparse. Sin embargo, una mejora es que la ruta desplegada mediante los comandos show incluye ahora detalles adicionales de la Access Control List (ACL, lista de control de acceso).

Enrutamiento optimizado del borde (OER, Optimized Edge Routing)

Ésta es una nueva característica en IOS versión 12.4 y se utiliza para determinar la mejor ruta saliente, generalmente cuando una organización cuenta con varias ISP. Esta característica se basa en NetFlow y el Service Assurance Agent (SAA, agente de aseguramiento del servicio). El OER detecta fallas en la ruta en el borde WAN y vuelve a enrutar en función a eso.

El OER también incluye una configuración de directiva, donde puede configurar directivas específicas y conmutar entre ellas.

Servicios IP

Los servicios IP incluyen gran variedad de mejoras, entre las que se incluyen:

- ▼ **Rate Based Satellite Control Protocol (RBSCP, protocolo de control satelital basado en la velocidad)** Proporciona optimizaciones para un vínculo satelital, que está planeado para reemplazar las Performance Enhancing Proxies (PEP, proxies de mejoramiento del rendimiento).
- ▲ **Listas de acceso IP** Soporta el filtrado de IP Options. Puede eliminar paquetes sellados o paquetes que utilicen IP Options (opciones de IP). También puede filtrar paquetes con base en las banderas TCP.

Instrumentación de la administración

Existe gran cantidad de nuevas SNMP Management Information Bases (MIB, bases de información para la Administración) de SNMP (para obtener mayor información acerca de las MIB, consulte el capítulo 13). Las características incluyen la cancelación de sesiones de configuración y el control fino sobre los subsistemas que pueden configurarse mediante el HTTP. Otras características son:

- ▼ **Cálculo del ancho de banda por medio de la tecnología Corvil** Es una tecnología QoS que cuenta con licencia para determinados enrutadores. Usted configura las SLA para que cuenten con niveles de pérdida de paquetes, retardo de enlaces y otro tipo de bases. El comando QoS muestra la interfaz de directivas y después muestra los niveles recomendados de ancho de banda.
- ■ **Egress NetFlow** Permite el rastreo de paquetes después de que han abandonado el enrutador. Se puede acceder a la información del NetFlow a través de una SNMP MIB.
- ■ **Configuración de reemplazo/retroceso** Es la joya de la corona en la instrumentación de la administración. Le permite enviar la configuración y, después, el enrutador genera una lista con las diferencias que usted puede revisar. Esta característica le permite retroceder el enrutador hasta la última configuración eficiente, si comete un error de configuración, puede retroceder a un estado funcional y tomar otra opción.
- ▲ **Administrador syslog insertado** Los mensajes syslog pueden personalizarse, enviarse a receptores específicos o correlacionarse con eventos en un dispositivo para limitar las tormentas de eventos.

QoS

La funcionalidad del QoS se fortaleció en la versión 12.4 del IOS. Además de la tecnología Corvil ya mencionada, gran cantidad de características mejoran el AutoQoS. Ahora los

administradores pueden desplegar la configuración AutoQoS recomendada que aplicaría la herramienta.

AutoQoS para la empresa rastrea las estadísticas de tráfico utilizando Network Based Application Recognition (NBAR, reconocimiento de la aplicación basada en la red), y después se genera una directiva QoS recomendada con base en esas mediciones.

La seguridad y las VPN

Otra adición significativa de la versión 12.4 del IOS, la característica de seguridad y VPN, hacen un total de 62 nuevas características. Algunas de las más importantes son:

- ▼ **Seguridad de Cisco y Router Device Manager (SDM, administrador de dispositivos de enrutador)** Combina el enrutamiento con la seguridad por medio de asistentes fáciles de usar y características para reparar fallas. Lo anterior también permite instituir directivas de sincronización del enrutamiento y de seguridad a través de la red.
- ■ **IPS transparente del IOS** Esta característica escanea el tráfico de las capas 2 y 3, permitiendo que el administrador despliegue el IPS en una red existente sin tener que alterar dispositivos direccionados estáticamente.
- ▲ **Interfaz de túnel virtual del IPSec** Ésta es una interfaz que soporta entunelamiento IPSec. Cuando se utiliza con Easy VPN, permite la creación dinámica de interfaces IPSec virtuales y permite el uso de grandes redes IPSec con una configuración mínima.

De ninguna manera ésta es una lista exhaustiva de las características del IOS versión 12.4, pero muestra algunas de las más importantes. Algunas de las nuevas características son más avanzadas y pueden pasar inadvertidas para un principiante. Sin embargo, si desea saber qué tipos de características se han incluido en la versión 12.4 del IOS, vaya al sitio www.cisco.com/go/ios. Esta página también detalla los avances y las características que se incluyen en IOS desde la publicación de este libro.

Conozca IOS XR

Mientras que el IOS de Cisco es la versión prevaleciente del sistema operativo de Cisco (sea desde 10.x hasta 12.x), Cisco ha creado también un nuevo sistema operativo que puede considerarse más modular. En mayo de 2004, Cisco lanzó el IOS XR para su plataforma CRS. Además de ese atractivo nombre (como lo debe ser todo nombre de un sistema operativo) el IOS XR promete más modularidad y características más allá de sus primeras versiones.

Modularidad

La característica más importante del IOS XR es su arquitectura modular, que ofrece mayor estabilidad y una administración más sencilla. Cisco está tomando con calma las transiciones. Por el momento, IOS XR sólo se utiliza en enrutadores tipo portadora, pero se podría esperar con certeza que algunas de las características tengan éxito en ambientes empresariales, suponiendo que existe una necesidad de negocios que las soporten.

Las versiones actuales del IOS funcionan como una sola pieza de código ejecutable en el enrutador. A medida que los clientes demandan diferentes características, éstas se agregan al sistema operativo. Esto significa que el código necesita más memoria y recursos del sistema para que se pueda ejecutar.

IOS XR está diseñado como servidor. Incorpora un sistema operativo y después se agregan los servicios como procesos independientes. Lo ideal es que esto hará que el sistema operativo sea más confiable y rápido.

El desplazamiento a nuevas arquitecturas del IOS comenzó a finales de 2004, cuando el IOS High Availability (IOS-HA, IOS de alta disponibilidad) se introdujo para el conmutador Catalyst 6500. Esta tecnología permite que los 6500 funcionen con tarjetas de supervisión doble y fallen sin perder paquetes o experimentar cualquier trastorno en la red. Esta tecnología ya se había utilizado en la serie 12000 de Cisco y está empezando a salir de la línea de productos de Cisco.

Velocidad y eficiencia

El cambio a esta arquitectura de sistema operativo diferente se debe a que cuantas más características se agregan al IOS, el sistema operativo se hace más grande y lento. Como tal, la arquitectura IOS XR puede incluir (o no) todas las características necesarias, lo que ofrece un sistema operativo más excitante y elegante. Las versiones actuales del IOS incluyen millones de líneas de código. El IOS XR tiene alrededor de 80 000.

Es estupendo tener todas las características del sistema operativo para poder solucionar cualquier problema en un dispositivo y poder decir, "Hey, hace todo esto…", pero la realidad es que la mayoría de los clientes no necesitan todas las características que el IOS ofrece. Todas esas características extra sólo hacen más lento el dispositivo.

Utilización de los comandos del IOS

Cualquier entorno de software de computadoras tiene sus peculiaridades y el IOS no es la excepción. Por un lado, IOS es un sistema operativo con un propósito específico al que se le ha quitado todo, excepto lo esencial, para hacer las cosas más simples y de una manera más rápida. Esto representa una buena opción, pero no podrá ver los atractivos que ofrece Mac, X-Windows (UNIX) o la interfaz gráfica de usuario (GUI) de Windows de Microsoft. Por otra parte, el IOS es uno de los sistemas operativos más importantes y ampliamente distribuidos en el mundo. Así que todo lo que necesita para operarlo está adentro, si lo busca.

La jerarquía de comandos del IOS

El IOS cuenta con cientos de comandos. Algunos pueden utilizarse en cualquier parte del IOS; otros sólo en un área específica. Ni siquiera los gurús de Cisco han memorizado todos los comandos del IOS. Así que, como cualquier buen sistema operativo, el IOS organiza sus comandos de manera jerárquica. En la figura 4-4 se muestra un panorama de la forma como están estructurados los comandos del IOS.

La primera división del IOS está entre los niveles User EXEC y Privileged EXEC del IOS. User EXEC sólo contiene, desde luego, un subconjunto de los comandos del Privileged EXEC. El modo User EXEC menos potente es donde residen los comandos **connect**, **login**, **ping**, **show** y otros, que son inocuos. Éstos también están en el Privileged EXEC, pero es en el modo privilegiado donde se encuentran los comandos más poderosos y posiblemente más destructivos (como **configure**, **debug**, **erase**, **setup** y otros), están disponibles de manera exclusiva.

Dependiendo del conjunto de características instaladas del IOS, existen muchos comandos más en Privileged EXEC que en el User EXEC. Los comandos en modo User EXEC

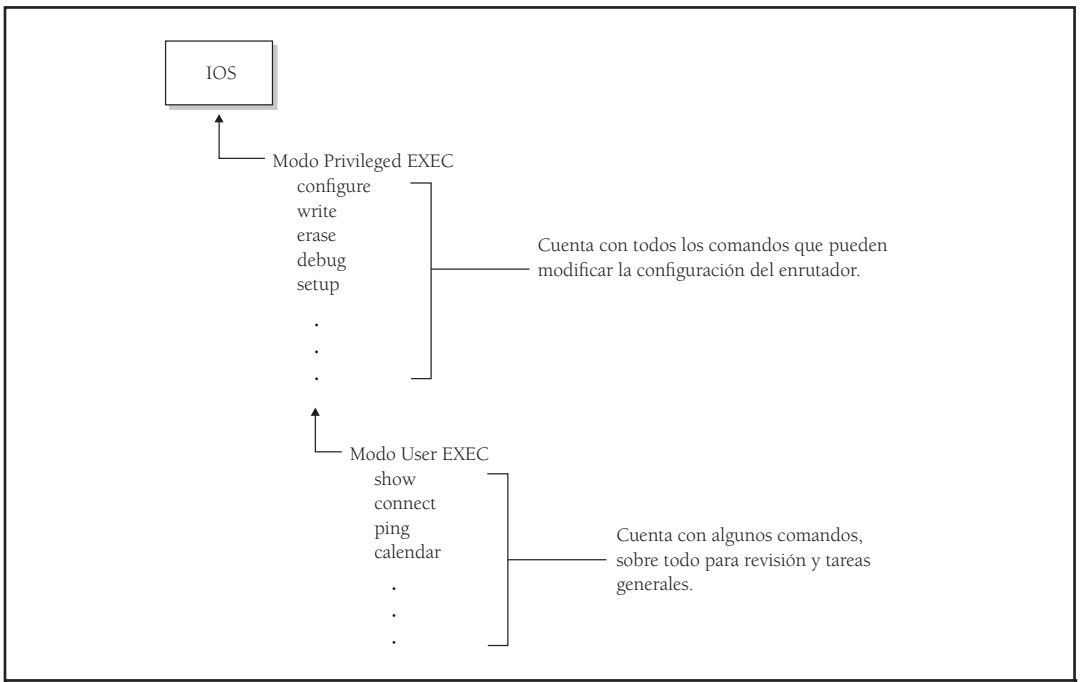


Figura 4-4. La estructura de comandos del IOS tiene dos modos.

tienden a ser "planos". En otras palabras, no tienen derivaciones que lleven a subconjuntos de comandos, como lo muestra el ejemplo siguiente:

```
Router>connect ?
  WORD  IP address or hostname of a remote system
  <cr>
```

Como regla, los comandos del modo User EXEC van, casi siempre, a sólo dos niveles de profundidad. Como es más potente, los comandos en el modo Privileged EXEC pueden ir más a fondo, como lo muestra la secuencia del ejemplo siguiente:

```
MyRouter#show ip ?
  access-lists         List IP access lists
  accounting           The active IP accounting database
  aliases              IP alias table
  arp                  IP ARP table
  .
  .
  .
```

El comando **show ip** tiene muchos argumentos (subcomandos) disponibles:

```
MyRouter#show ip arp ?
H.H.H                48-bit hardware address of ARP entry
Hostname or A.B.C.D  IP address or hostname of ARP entry
```

```
  Null                  Null interface
  Serial                Serial
  Ethernet             IEEE 802.3
  <cr>
```

Los argumentos pueden ser modificados, aún más a fondo, por otros argumentos en el árbol de "subcomandos" del comando raíz:

```
My Router#show ip arp serial ?
   <0-3>  Serial interface number
   <cr>
```

Por ejemplo, después de que ha agrupado todo un comando a partir de las opciones anteriores (**ip access-lists serial2**, por ejemplo) ingresaría un retorno de carro después del "2" para el número de línea serial 2.

Armar líneas de comandos directamente es simple. La parte truculenta del asunto es saber dónde encontrar argumentos para los comandos raíz, de tal forma que pueda agrupar líneas de comandos completas, y correctas. Aquí es donde el sistema de ayuda del IOS entra en acción.

Recorrido del IOS con el sistema de ayuda

El IOS cuenta con un sistema de ayuda integrado que es sensible al contexto. Esta última característica significa que el sistema de ayuda responde con información basada en la parte en que se encuentra dentro del sistema en ese momento. Puede obtener el tipo de ayuda sensible al contexto más general con sólo ingresar un signo de interrogación cuando el sistema solicite que ingrese un comando. Por ejemplo, a continuación se muestra una lista de todos los comandos raíz disponibles en el nivel User EXEC del IOS:

```
Router>>?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  atmsig           Execute Atm Signaling Commands
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lat              Open a lat connection
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
.
.
.
```

También puede obtener lo que se llama "ayuda con una palabra" ingresando parte del comando que no conozca, seguido de un signo de interrogación:

```
Router>>sh?
show
```

La ayuda con una palabra representa una gran ayuda para obtener definiciones y está muy a la mano para investigar qué son los comandos truncados, como en el caso del comando show del ejemplo anterior. Otra forma de obtener ayuda con un comando parcial es simplemente ingresarlo; el sistema regresará con una instrucción sobre la manera de obtener una ayuda completa acerca del comando:

```
Router>>sh
% Type "show ?" for a list of subcommands
```

Observe que en el comando **show ?** sugerido de la ayuda, existe un espacio entre el comando y el signo de interrogación. Como ya habrá notado, siempre hay un espacio entre un comando y su modificador (llamado argumento). Para solicitar una lista de argumentos disponibles para el comando debe hacer lo anterior en una solicitud de ayuda. En el ejemplo siguiente, el signo de interrogación solicita todos los argumentos disponibles del comando **show**:

```
Router>>show ?
  bootflash      Boot Flash information
  calendar       Display the hardware calendar
  clock          Display the system clock
  context        Show context information
  dialer         Dialer parameters and statistics
  history        Display the session command history
  hosts          IP domain-name, lookup style, nameservers,
                          and host table
  kerberos       Show Kerberos Values
  location       Display the system location
  .
  .
  .
```

A veces, esta forma de utilizar ayuda se llama ayuda de sintaxis de comando, porque le ayuda a completar correctamente un comando con muchas partes. La ayuda de sintaxis de comando es una herramienta de aprendizaje muy poderosa, porque proporciona una lista de palabras clave o argumentos disponibles en casi cualquiera de las operaciones del comando IOS. Recuerde que el espacio debe insertarse entre el comando y el signo de interrogación para usar la ayuda de sintaxis de comando.

En el IOS, la ayuda juega un papel más importante que en los sistemas de ayuda de las PC normales o de los paquetes de software de aplicaciones de negocios. Esos sistemas de ayuda, que también son sensibles al contexto, son en esencia manuales en línea que tratan de ayudarle a aprender toda una subsección de la aplicación. La ayuda que proporciona el IOS es simple: solamente desea llevarlo a la línea de comando siguiente. Eso es reconfortante. Casi todos los sistemas de ayuda actuales parecen suponer que está ansioso de invertir horas leyendo toda la información acerca de un subsistema completo cuando, en realidad, sólo desea saber qué hacer en ese momento.

NOTA No se confunda con el nombre del comando **show**; despliega información acerca del sistema que se está ejecutando. No es un comando de varios propósitos para "mostrar" información de ayuda; el comando **?** lo hace. El comando **show** se utiliza para examinar el estado del enrutador.

Sintaxis de comandos

La operación de los comandos del IOS es más compleja que el simple recorrido por el árbol de subcomandos del comando raíz. Para ejecutar el IOS, debe aprender a combinar diferentes comandos (no únicamente a modificar un solo comando) con el fin de formar las líneas de comando que harán el trabajo pesado que la administración de la red requiere. Sin embargo, el IOS no es cosa del otro mundo, como lo demuestra la secuencia de ejemplo siguiente:

```
MyRouter#config
Configuring from terminal, memory, or network [terminal]?
```

En el anterior indicador de comandos, estamos ingresando al modo config, y el IOS desea saber si la configuración se entregará a través de una descarga de la red, se copiará de una imagen almacenada en la memoria NVRAM del enrutador o se ingresará desde la terminal. Pudimos simplemente haber omitido el indicador al unir los dos comandos en una sola línea de comandos:

```
MyRouter#config terminal
```

No deje que esto lo confunda: no estamos configurando una terminal, como parecen indicarlo las letras IOS. En la escritura abreviada del IOS, **config terminal** significa "configuración desde una terminal". El paso siguiente es "apuntar" a lo que se va a configurar. Vamos a configurar una interfaz:

```
MyRouter(config)#interface
% Incomplete command.
```

En lugar de preguntar, "¿Qué interfaz quisiera configurar?", el IOS contesta de manera ruda que nuestro comando no es válido. Aquí es donde se requiere parte de la experiencia del usuario:

```
MyRouter(config)#interface fastethernet 0
MyRouter(config-if)#
```

El IOS deseaba saber qué modulo de interfaz física se iba a configurar. Una vez indicado que el puerto 0 del módulo de interfaz Fast Ethernet era el que se iba a configurar, la solicitud del IOS cambia a My Router(config-if)#, donde "if" es la forma abreviada de "interfaz". (Los modos de configuración se estudiarán más adelante en este capítulo.)

NOTA Siempre mantenga un registro del dispositivo al que esté apuntando cuando lleva a cabo una configuración. La solicitud IOS config es genérica y no le dice a qué interfaz de red está apuntando la indicación (config-if)#. El IOS no inserta el nombre de la interfaz en la indicación.

Una vez que haya apuntado a la interfaz de red que configurará, desde ahí la configuración del enrutador es sólo cuestión de proporcionar al IOS los parámetros de configuración para esa interfaz, misma que estudiaremos unas páginas más adelante.

Para que cualquier persona pueda comenzar a ingresar líneas de comando (con algo de tiempo y trabajo duro, por supuesto) basta con que comprenda cómo funciona la sintaxis del IOS, combinada con el sistema de ayuda.

Finalización de comandos

Tarde o temprano encontrará las líneas de comando del IOS llenas de símbolos aparentemente crípticos. No se sienta intimidado; son sólo comandos que los usuarios expertos han truncado (cortado en su parte final) para acelerar el proceso de teclear comandos y, quizás, impresionar un poco a la gente. El IOS es como el DOS y casi todos los demás editores, en el sentido de que aceptan comandos truncados. Sin embargo, si el comando truncado no es una secuencia de letras única al conjunto de comandos, generará un comando de error. Por ejemplo, si teclea las primeras dos letras de un comando con el que otro comando comienza, obtendrá un mensaje de error como el siguiente:

```
Router#te
% Ambiguous command:  «te»
```

Este error aparece porque el IOS cuenta con tres comandos que comienzan con la secuencia de letras te: **telnet**, **terminal** y **test**. Si la idea fue enviar un Telnet a alguna parte, un carácter adicional hará la tarea:

```
Router>>tel
Host:
```

NOTA Si se le interpone un comando truncado que no entienda, simplemente consulte su significado utilizando la ayuda en el sistema de ayuda en línea. Teclee el comando truncado seguido del signo de interrogación. A diferencia de la ayuda de sintaxis de comando, cuando utilice la ayuda, no debe ir espacio alguno antes del comando **?**

Recuperación del historial de un comando

El IOS conserva un historial de los comandos ingresados más recientemente al sistema. La capacidad de almacenar comandos es útil para:

- ▼ No tener que teclear comandos que se ingresan de manera repetida.
- ▲ No tener que recordar largas y complicadas líneas de comando.

La utilidad del historial mantendrá un registro de todo lo que ingrese al sistema, incluidos los comandos erróneos. El único límite es la cantidad de memoria de almacenamiento que se asigne para conservar el historial. Aquí se muestra un ejemplo:

```
Router#show history
  test
  tel
  exit
  enable
```

Los comandos ingresados más recientemente se encuentran en la parte superior de la lista del historial. Los comandos no se encuentran en orden alfabético.

Las teclas de flecha también pueden utilizarse para desplegar comandos anteriores. El uso de las teclas de flechas evita ingresar el comando del historial show, pero sólo muestra los comandos anteriores de uno en uno. Presione la tecla de flecha hacia arriba (o Ctrl-P) para recordar los comandos más recientes. Si ya se encuentra en algún punto de la secuencia de comandos anteriores, presione la tecla de flecha hacia abajo (o Ctrl-N) para recordar los comandos menos recientes.

Revisión general de los modos del enrutador

Los enrutadores de Cisco pueden estar en cualquiera de los siete posibles modos de operación, como se muestra en la figura 4-5. Tres de ellos son modos de arranque. En los otros cuatro, los administradores de red se encuentran en el modo User EXEC o Privileged EXEC (habilitado). Una vez dentro del Privileged EXEC, se pueden hacer cambios de configuración ya sea a todo el dispositivo o a una interfaz de red específica.

Debe mantener un registro del modo en que se encuentra el enrutador en todo momento. Muchos comandos del IOS sólo se ejecutarán desde un modo específico. Como se observa en la figura 4-5, los modos del enrutador se hacen más específicos, y poderosos, a medida que el usuario se mueve hacia el centro del IOS. Vale la pena echarle un vistazo a las indicaciones del IOS, porque siempre le indicarán en qué modo se encuentra.

Los tres tipos de modos de operación

Los modos de operación del enrutador Cisco están diseñados para llevar a cabo tres tareas generales:

- ▼ Arrancar un sistema.
- ■ Definir los comandos que pueden utilizarse.
- ▲ Especificar la parte o las partes del enrutador que se verán afectados por los cambios realizados al archivo config.

En la tabla 4-1 se muestran los diferentes modos del IOS y para qué se utilizan. A medida que se familiarice con la conectividad Cisco en general, y con el software IOS en particular, podrá observar que la mayor parte de los movimientos se llevan a cabo dentro de los diferentes modos de configuración.

Modos de configuración

Los modos de configuración difieren de los modos de usuario por su naturaleza. Los dos modos EXEC definen el nivel de comandos IOS que puede utilizar. En contraste, los modos de configuración se utilizan para atacar interfaces de red específicas (físicas o virtuales) a las que se aplica un cambio de configuración. Por ejemplo, podría ir al modo de configuración de interfaz [identificado por (config-if)#] para configurar un módulo específico de interfaz Ethernet. Existen docenas de modos de configuración, cada uno de ellos para partes diferentes del archivo de configuración. En la tabla 4-2 se proporciona una lista de los ocho modos de configuración más comunes.

Una mirada a la tabla 4-2 le indica que el modo de configuración se relaciona tan sólo con instruir al IOS lo que debe hacer con los paquetes que están fluyendo por el dispositivo.

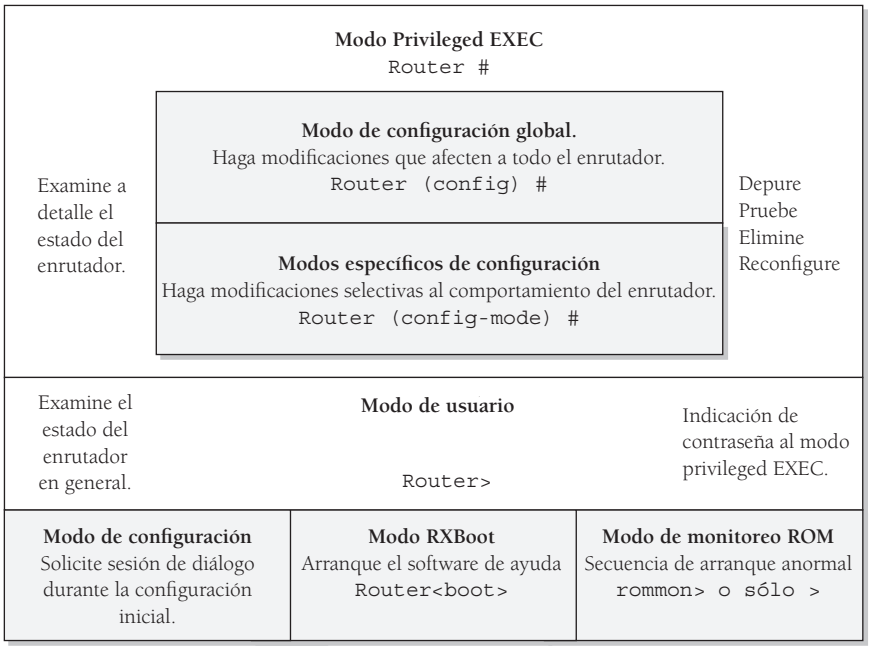


Figura 4-5. Siete modos de operación son posibles en los enrutadores Cisco.

Algunos modos se aplican a los paquetes que fluyen a través de puntos de conexión específicos, como interfaces, líneas y puertos. Los demás modos de configuración del IOS tienen que ver con protocolos y tablas de enrutamiento necesarias para manejar dicho flujo.

Tipo de modo	Propósito
Arranque	El *modo de configuración* es utilizado para crear un archivo de configuración de trabajo básico. El *modo RXBoot* ayuda al enrutador a arrancar el sistema operativo a un estado rudimentario cuando la imagen del IOS no puede encontrarse en la memoria flash. El *modo de monitoreo ROM* es utilizado por el enrutador si la imagen del IOS no puede encontrarse o si la secuencia de arranque normal se interrumpió.

Tabla 4-1. Tres tipos generales de modos del software IOS (*continúa*).

Tipo de modo	Propósito
Usuario	El *modo User EXEC* es el primer "cuarto" al que uno entra después de acceder al sistema; restringe a los usuarios el acceso a examinar el estado del enrutador.
	El *modo Privileged EXEC (Privileged EXEC Mode)* se ingresa utilizando una contraseña Enable; permite a los usuarios modificar el archivo config, borrar la memoria, etcétera.
Configuración	El *modo de configuración global* cambia los parámetros de todas las interfases.
	El *modo de comando Config* "se encarga" de cambios en interfaces específicas.

Tabla 4-1. Tres tipos generales de modos del software IOS (*conclusión*).

Los dos tipos de archivos config

Existen dos tipos de archivos config para cada enrutador: running-config y el startup-config. Como sus nombres lo indican, la diferencia básica es que el archivo running-config está "vivo" en el sentido de que está funcionando en la RAM. Cualquier cambio que se le haga al archivo se aplica de inmediato. El archivo startup-config se almacena en la NVRAM del enrutador, donde el programa de arranque del IOS se dirige a consultar los parámetros de la configuración funcionando en el enrutador cuando se arranca.

Modo de configuración	Puerto de destino del enrutador	Se aplica a
Global	Router(config)#	Todo el archivo config.
Interfaz	Router(config-if)#	Módulo de la interfaz (físico).
Subinterfaz	Router(config-subif)#	Subinterfaz (virtual).
Controlador	Router(config-controller)#	Controlador (físico).
Global	Router(config)#	Todo el archivo config.
Interfaz	Router(config-if)#	Módulo de la interfaz (físico).
Subinterfaz	Router(config-subif)#	Subinterfaz (virtual).
Controlador	Router(config-controller)#	Controlador (físico).

Tabla 4-2. Los modos de configuración y las partes del enrutador de destino.

Después de cambiar los parámetros específicos del enrutador, el comando **copy** se utiliza para guardar y distribuir los cambios en el archivo config. Como se observa en la parte inferior de la figura 4-6, un archivo config maestro puede distribuirse a otros enrutadores a través de un servidor TFTP.

COMANDOS BÁSICOS DEL ENRUTADOR

Algunos comandos raíz principales manejan la mayor parte de las tareas relacionadas con la configuración de los enrutadores. Entre ellos se encuentran los siguientes:

- **show** Examina el estado del enrutador.
- **configure** Hace modificaciones en los parámetros del archivo config.
- **no** Niega el valor de un parámetro.
- **copy** Lleva a cabo los cambios en el archivo config.

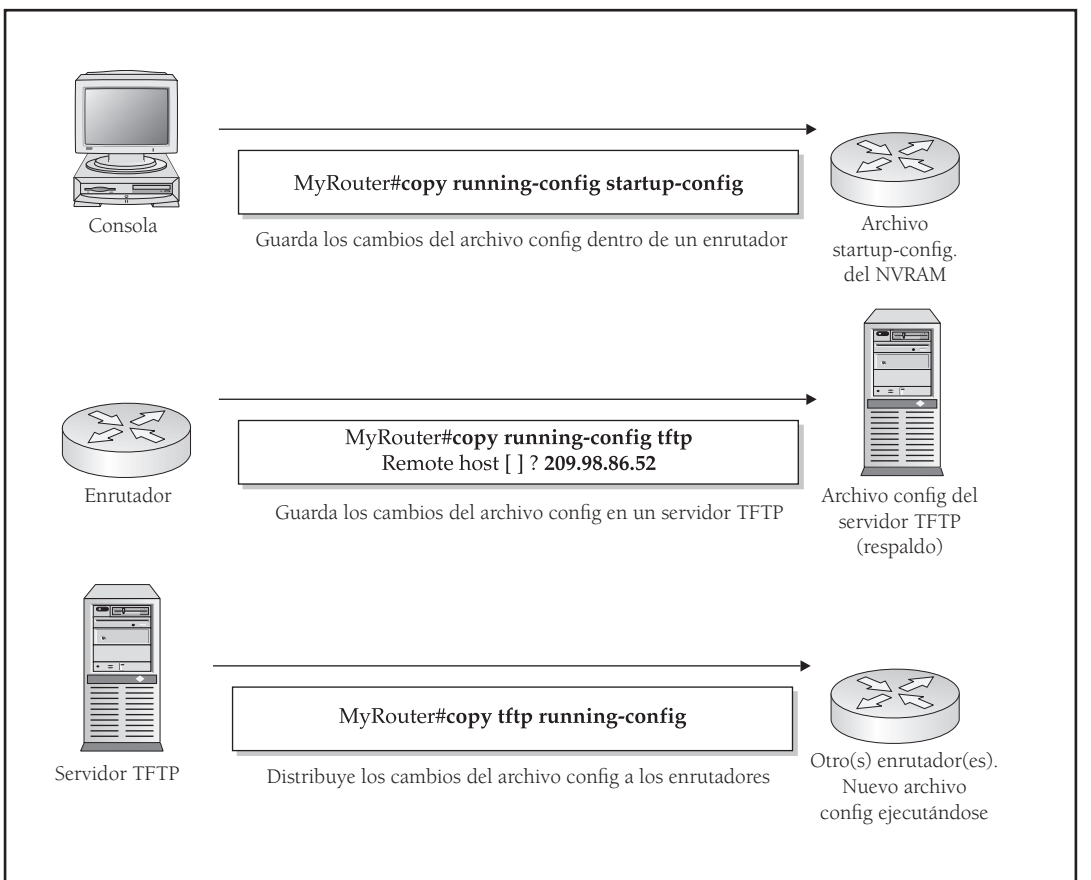


Figura 4-6. Los archivos running-config y startup-config se utilizan de diferentes maneras.

El comando **show** es la base del IOS. Se utiliza para examinar casi todo acerca de un enrutador y su configuración. El siguiente ejemplo muestra quiénes han iniciado sesión en el enrutador, que presenta información momento a momento:

```
Router>>show users
    Line     User      Host(s)              Idle Location
*  2 vty 0             idle                  00:00:00
```

El comando **show** también se puede utilizar para desplegar información, como la versión del software IOS instalado:

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-ADVIPSERVICESK9-M), Version 12.3(18),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 15-Mar-06 14:16 by dchih
Image text-base: 0x80008098, data-base: 0x81DD1190

ROM: System Bootstrap, Version 12.2(7r) [cmong 7r], RELEASE SOFTWARE (fc1)
ROM: C2600 Software (C2600-ADVIPSERVICESK9-M), Version 12.3(18), RELEASE
SOFTWARE (fc3)
System returned to ROM by power-on
System image file is “flash:c2600-advipservicesk9-mz.123-18.bin”
```

El comando **no** se utiliza para revertir el valor de un parámetro. Por ejemplo, si activa la contabilidad IP para el puerto 1 de Fast Ethernet y ahora desea desactivarla, apunte a esa interfaz en el modo de interfaz de configuración, que se muestra con el indicador de comandos MyRouter(config-if)#, y después simplemente incluya antes del comando para activarlo (**ip accounting**), el comando **no**, como se muestra a continuación:

```
MyRouter(config-if)#no ip accounting
```

Cualquier comando del IOS puede desactivarse utilizando la sintaxis del comando **no**.

Si sabe cómo navegar dentro de un entorno de sistema operativo siempre tendrá ganada la mitad de la batalla. Esto es especialmente válido en las interfaces de línea de comandos, porque no existen íconos gráficos que muestren el camino. En la tabla 4-3 se muestra una lista de los comandos que se utilizan para moverse en el ambiente del IOS.

Los comandos “abreviados” son de gran utilidad, porque algunas líneas de comandos del archivo config pueden hacerse complejas y de gran tamaño.

CONFIGURACIÓN PASO A PASO DE UN ENRUTADOR

Un enrutador puede configurarse mediante una de las opciones siguientes:

- Ingresando los cambios directamente al archivo running-config en el enrutador.

- Descargando un nuevo archivo config de un servidor TFTP.
- Configurando el archivo config desde el principio.

La mejor forma de aprender a configurar un enrutador es configurar uno desde el principio. Pasaremos al modo de configuración aquí, no porque se lleve a cabo el procedimiento con mucha frecuencia, sino porque es una excelente forma de revisar los fundamentos de la configuración del enrutador.

Modo de configuración

En esencia, la configuración es una secuencia de comandos interactivos que se ejecutan para inicializar el enrutador a un nivel básico de operación. Si el dispositivo es nuevo (y, por tanto, nunca se ha configurado), o si se destruyó el archivo config del NVRAM, el software IOS va al modo de configuración, como opción predeterminada, para reconstruir el archi-

Comando	Propósito
Enable	Mover del modo User EXEC al Privileged EXEC.
Disable	Regresar del modo User EXEC al Privileged EXEC.
Exit	Salir del modo de configuración o terminar una sesión activa.
CTRL-A	Desplazarse al inicio de una línea de comandos.
CTRL-B	Desplazarse hacia atrás un carácter.
CTRL-F	Desplazarse hacia delante un carácter.
CTRL-Z	Salir o abandonar un proceso (como un acceso o un desplegado de varias páginas).
ESC-B	Desplazarse al principio de la palabra anterior (sirve para hacer correcciones).
ESC-F	Desplazarse al comienzo de la próxima palabra.

Tabla 4-3. Comandos de navegación del IOS.

vo config desde el principio. Una vez realizado lo anterior, puede abandonarse el modo de configuración y el enrutador arrancará en el modo IOS normal, donde se puede construir un archivo config completo. El modo de configuración no se ejecuta solo; debe estar presente un administrador de redes para responder una larga secuencia de preguntas acerca de la configuración del enrutador. Asimismo, como el enrutador no está configurado, no puede ejecutar la configuración a través de una conexión a la red. La configuración debe ejecutarse mediante el puerto de la consola o del puerto AUX.

No es necesario que un enrutador sea nuevo o falle para tener que ejecutar el programa de configuración. La configuración también puede ser útil en situaciones que no sean de emergencia. A menudo, los administradores de red utilizan la configuración cuando un archivo config se ha hecho tan confuso que es mejor empezar desde cero (como si fuera una hoja en blanco). Utilizándolo de esta forma, los valores de los parámetros dados como respuestas durante una sesión de configuración sobrescriben la información en el archivo config existente.

El modo de configuración se ingresa utilizando el comando setup. Sin embargo, antes de comenzar, conecte el puerto COM de su PC al puerto console del enrutador. Después arranque cualquier software de emulación que prefiera utilizar (recuerde que estará iniciando sesión en el sistema operativo del enrutador y no en el de su PC). Las instrucciones siguientes suponen que está trabajando en una PC con Microsoft Windows. Si no es así, necesitará saber cómo arrancar su emulador de terminal. Esto no debe representar un problema, porque si está trabajando en una Apple, usted es un sobreviviente; si está ejecutando X-Windows desde una computadora UNIX, en primer lugar, no necesitará nuestro consejo acerca de ese problema trivial:

1. Haga clic en el botón **Inicio**.
2. Seleccione **Programas** | **Accesorios** | **Comunicaciones** | **HyperTerminal**.
3. Se abrirá una ventana HyperTerminal y aparecerá un cursor parpadeante en la esquina superior izquierda.
4. Ingrese el nombre de la conexión que desea realizar.
5. Seleccione **TCP/IP** del menú contextual.
6. Ingrese la dirección IP del enrutador y el puerto de conexión.
7. Presione ENTER y deberá ver el indicador de comandos del enrutador.
8. Vaya al modo Privileged EXEC ingresando el comando enable y, después, la contraseña Enable Secret password (setup es, en esencia, un comando de configuración, y los archivos config no pueden modificarse a partir del nivel User EXEC del IOS).
9. Teclee setup e iniciará el modo de configuración (setup mode).

Una vez que el modo de configuración ha iniciado, aparecerá un anuncio con instrucciones de comando, una opción para abandonar el sistema y otra para revisar un resumen de los módulos de interfaz en el enrutador.

```
The following code Router#set
*Mar  3 04:58:46.167: %SYS-5-CONFIG_I: Configured from console by conso-
leup


         --- System Configuration Dialog ---
```

```
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:

  Enter host name [Router]:
```

Si decide seguir adelante, la configuración arranca configurando los parámetros globales, que son información básica como el nombre del enrutador y las contraseñas. En caso de que sea un enrutador nuevo o que se haya destruido el archivo config del NVRAM, debe ingresar nuevos parámetros para estas cosas, como se muestra en la siguiente secuencia:

```
Configuring global parameters:

  Enter host name [Router]: MyRouter

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: test

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: test1
```

Si observa detenidamente el ejemplo siguiente, notará que la configuración detecta automáticamente módulos de interfaz físicamente presentes en las ranuras del enrutador. La configuración presenta las interfaces disponibles y solicita la que deseamos utilizar para conectarnos a la red de administración. En este caso, hemos elegido la conexión Fast Ethernet.

```
Current interface summary


Interface        IP-Address      OK? Method Status
Protocol
FastEthernet0/0  unassigned      YES unset  administratively down down
```

```
Serial0/0        unassigned      YES unset  administratively down down
Serial0/1        unassigned      YES unset  administratively down down

Enter interface name used to connect to the
management network from the above interface summary: FastEthernet0/0

Configuring interface FastEthernet0/0:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]:
  Configure IP on this interface? [no]:
```

Una vez que haya realizado esta selección, el enrutador muestra la secuencia de comandos completa. Se generó la siguiente secuencia de comandos de configuración:

```
hostname MyRouter
enable secret 5 $1$gAi3$BXI873YTi..MOL0NIl5X11
enable password test1
line vty 0 4
password test2
no snmp-server
!
no ip routing

!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
half-duplex
no ip address
no mop enabled
!
interface Serial0/0
shutdown
no ip address
!
interface Serial0/1
shutdown
no ip address
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
```

Si sigue adelante, la configuración toma algunos segundos para "construir" el archivo config (como se mencionó antes, los archivos config no se editan de manera interactiva, como un archivo de procesador de palabra). Una vez que se ha construido el archivo config, se le envía al IOS en "modo normal" y se le aconseja que si desea continuar configurando, debe hacerlo utilizando el comando **config**:

```
[OK]
```

Una vez que se haya terminado la sesión de configuración, se habrá creado un archivo básico de configuración. A partir de ahí, puede seguir el procedimiento normal y utilizar el comando **configure** para ingresar un archivo de configuración completo.

Asignación de una identidad a un enrutador

Tomarse el tiempo para asignar un nombre a cada enrutador y documentarlo adecuadamente facilita la administración de las redes. La información de identificación puede asignarse al:

- ▼ Proporcionar al enrutador un nombre significativo.
- ■ Documentar las interfaces del enrutador de forma individual.
- ▲ Escribir un mensaje del día en el enrutador (MOTD).

Podrá observar con frecuencia que el nombre "Router" (enrutador) se utiliza en los ejemplos de configuración. No permita que esto lo confunda; "Router" no es una parte obligatoria de la indicación del IOS de Cisco. Un enrutador puede llamarse "MainOffice" o "R23183" o de cualquier otra forma. A los enrutadores se les deben asignar nombres llenos de significado que les informen a los administradores de redes dónde está el enrutador y qué hace. Debe estar en el modo de configuración global y utilizar el comando **hostname** para modificar el nombre del dispositivo, como se muestra aquí:

```
Router(config)#hostname MyRouter
MyRouter(config)#
```

Debido a que el nuevo nombre se ingresó en el archivo running-config, se utiliza el nuevo nombre de enrutador MyRouter inmediatamente en el siguiente indicador de comandos. Sin embargo, a menos que utilice los comandos write o copy para almacenar el nuevo nombre (o cualquier otro cambio) en NVRAM, si el enrutador fue reiniciado, el IOS debería venir respaldado con el viejo nombre.

NOTA El término "host" puede causar confusión a los veteranos de la industria de la computación pero nuevos en el campo de la interconectividad. En el mundo de las aplicaciones de cómputo, un anfitrión es un sistema de cómputo completo que trabaja como servidor y los dispositivos de red son nodos. En el contexto de la interconectividad, host puede significar cualquier dispositivo de red, incluidos enrutadores, conmutadores y servidores de acceso, además de servidores. Tratamos de mantener esto claro denominando "hosts" sólo a las computadoras y llamando al equipo de red "dispositivos" (pero tenga cuidado, el término "host" puede tener diferentes significados en los documentos de interconectividad).

Una interfaz de enrutador puede documentarse específicamente utilizando el comando **description**. El uso de descripciones es una formidable manera de mantener un registro de la red (y de los usuarios) que gozan de los servicios de una interfaz. Tal vez esto no suene muy importante, pero las redes grandes cuentan con miles de interfaces, y éstas se reconfiguran muy a menudo. Para ingresar una descripción específica de una interfaz, primero debe ir a ella, en este ejemplo, FastEthernet0/0:

```
MyRouter(config)#interface FastEthernet0/0
MyRouter(config-if)#
```

Luego ingrese el comando description seguido de la descripción:

```
MyRouter(config-if)#description Fast Ethernet for finance department
MyRouter(config-if)#
```

Las descripciones pueden ser de hasta 240 caracteres de longitud. Para cerrar el bucle, la descripción puede verse en una parte del archivo config de la interfaz:

```
MyRouter(config-if)#
MyRouter#show running-config
.
.
.
interface FastEthernet0/0
 description Fast Ethernet for finance department
```

Únicamente los administradores de red pueden ver los nombres de los enrutadores y las descripciones de la interfaz. Una tercera herramienta para la identificación de un enrutador (el anuncio mensaje de día) es una forma para enviar anuncios a todas las terminales que estén conectadas a un enrutador. Los enrutadores MOTD (Message of The Day) son una buena forma de asegurarse de que los anuncios de mantenimiento sean vistos por todos los usuarios de la red. Los anuncios suelen utilizarse para prevenir en contra de usos no autorizados, para anunciar la programación de los tiempos en que la red no estará disponible, y para otro tipo de anuncios. Utilice el comando **banner motd** para desplegar un anuncio en un enrutador:

```
MyRouter(config)#banner motd $MyRouter will be down tonight$
```

El signo de dólares se seleccionó arbitrariamente para utilizarse como delimitador de comienzo y final del mensaje del anuncio. Puede utilizarse cualquier carácter; solamente asegúrese de utilizar uno que no aparezca en el texto del anuncio en sí.

El anuncio se desplegará siempre que alguien ingrese directamente al enrutador o quiera acceder al enrutador desde un navegador Web:

```
MyRouter will be down tonight
User Access Verification
Password:
```

Los anuncios atractivos con varias líneas pueden crearse utilizando comandos en modo extendido para las terminales VT. El VT es una estándar *de facto* para la programación de terminales de Digital Equipment Corporation (en la actualidad, parte de Compaq Computer).

PRECAUCIÓN No coloque información delicada en los anuncios MOTD, porque cualquiera puede verlos. Además, podría haber implicaciones legales y de seguridad si un mensaje "Bienvenido a…" saluda a un hacker que está tratando de entrar a su red.

Examen del estado de un dispositivo

El análisis de las interfaces de red es una técnica básica para obtener información crítica sobre el estado de la red. El comando **show interface** lo hace. En la figura 4-7 se muestra una salida como ejemplo.

Los mensajes con señales de presencia son enviados por las interfaces entre sí en el nivel de la capa de enlace de datos para confirmar que el circuito virtual entre ellos aún está activo.

En la tabla 4-4 se muestra un resumen del significado de los diferentes reportes de estado (utilizando como ejemplo una interfaz llamada Ethernet1).

Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco)

Cisco cuenta con una herramienta de propietario para la reparación de fallas llamada Cisco Discovery Protocol (CDP). Se incluye en todos los equipos de Cisco, incluidos los enrutadores. El CDP lo utilizan los dispositivos para descubrir y aprender acerca de sí mismos. Es independiente de los medios y los protocolos. Los dispositivos Cisco utilizan el CDP como una forma de anunciar a los vecinos de su existencia en una LAN o en el extremo lejano de una WAN. Piense en el CDP como un tipo de comando "show configuration" para un grupo de enrutadores Cisco y otros dispositivos (una forma para que los dispositivos le informen a cualquiera que llegara a escuchar acerca de su versión, tanto de software como de hardware), nombre de anfitrión (host), número y tipo de información de interfaz (dirección IP, duplex, dominio VTP, alimentación tomada de la VLAN).

El CDP funciona en la capa de vinculación de datos con la finalidad de ser compatible con los dispositivos que trabajan sobre diferentes protocolos de la capa de red (IPX, IP, AppleTalk, etcétera). El CDP puede comunicarse con cualquier medio físico que soporte el Subnetwork Access Protocol (SNAP, protocolo de acceso a la subred), incluidos LAN, Frame Relay y ATM. El SNAP es un protocolo diseñado para que los dispositivos envíen mensajes dentro de una subred, permitiéndoles que mantengan un registro de los dispositivos que se encuentran trabajando en el grupo.

El CDP es automático. Puede conectar cualquier combinación de dispositivos de Cisco, alimentarlos con energía eléctrica, mantenerlos alejados y dejar que se identifiquen entre sí (aunque lo anterior suceda antes de asignarse direcciones de red). El CDP puede hacer lo anterior utilizando un estándar propietario llamado Cisco Proprietary Data-Link Protocol (protocolo de propietario de vinculación de datos de Cisco). En la figura 4-8 se muestra cómo el CDP mantiene unidos a los protocolos incompatibles.

El IOS reporta el estado de "up/down" de cada interfaz del enrutador.

```
Serial1 is administratively down, line protocol is down
.
.
.
Serial2 is administratively down, line protocol is down
.
.
.
TokenRing0 is administratively down, line protocol is down
.
.
.
```

El IOS sabe si la línea está funcionando mediante la verificación de una señal portadora.

Por medio de la verificación de los mensajes de presencia se determina si el protocolo de línea se encuentra funcionando.

```
TokenRing1 is up, line protocol is up

Hardware is TMS380, address is 0006.clde.4ab9 (bia 0006.clde.4ab9)
Internet address is 10.1.13.10/24
MTU 4464 bytes, BW 16000 Kbit, DLY 630 usec, rely 255/255, load 1/255
Encapsulation SNAP, loopback not set, keepalive set (10 sec)
ARP type:  SNAP,  ARP Timeout 04:00:00
Ring speed: 16 Mbps
```

Figura 4-7. El comando show interface reporta información actual.

El CDP está habilitado en forma predeterminada en todos los dispositivos de Cisco. Este protocolo trabaja permitiendo que todos los dispositivos Cisco de una red conectada transfieran directamente marcos CDP entre sí. La clave para la comprensión del límite exterior del CDP reside en las palabras "conectado directamente". El CDP puede descubrir dispositivos más allá de una LAN, pero sólo si la conexión WAN no pasa por ningún dispositivo que no sea Cisco (y, por ende, que no trabaje con el CDP) para hacer la conexión. Los marcos del CDP deben pasar a través de las conexiones de interconexión para seguir extendiendo el mapa de lo que está conectado a la LAN base.

Mensaje	Significado
Ethernet1 is up, line protocol is up	Funcionando correctamente.
Ethernet1 is up, line protocol is down	Interfaz correcta, pero no hay conexión activa.
Ethernet1 is down, line protocol is down	Problema de interfaz.
Ethernet1 is administratively down, line protocol is down	Deshabilitado.

Tabla 4-4. Definiciones acerca del informe de estado de la interfaz.

Protocolos de alto nivel	TCP/IP Novell Apple Talk DECnet Otros IPX
Cisco Proprietary Data-Link Protocol	Descubre a otros dispositivos de Cisco, despliega información acerca de ellos
SNAP	Ethernet Token Ring ATM Otros relevadores

Figura 4-8. El CDP evita protocolos incompatibles para mantener un registro de las redes.

Utilice el comando **show CDP** para ver cuáles son sus parámetros operativos actuales.

```
MyRouter>show CDP
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
```

La solicitud de ayuda de sintaxis de comandos para el comando **show CDP** despliega el tipo de información que el CDP puede proporcionar:

```
MyRouter>show CDP ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  <cr>
```

El uso más común del CDP es desplegar otros dispositivos directamente conectados al que solicita información acerca del CDP:

```
vsigate>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge, S - Switch, H - Host, I - IGMP, r - Repeater

Device ID          Local Intrfce      Holdtme     Capability
Platform              Port ID
tacacsrouter           Fas 0            168            R
3640                   Fas 0
Switch.velte.com       Eth 1            129            S
WS-C2924M              Fas 0/1
vsitest7               Fas 1            169            R
RSP2                   Fas 6/0
```

Para ver un vecino específico con más detalle, utilice el comando **show cdp entry**:

```
vsigate>show cdp entry vsitest7
-------------------------
Device ID: vsitest7
Entry address(es):
  IP address: 10.1.12.2
Platform: Cisco RSP2,  Capabilities: Router
Interface: Ethernet1,  Port ID (outgoing port): Ethernet6/0
Holdtime : 138 sec

Version :
Cisco IOS Software, 3600 Software (C3640-JK9O3S-M), Version 12.4(3b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 08-Dec-05 22:10 by alnguyen
```

Como observará, el CDP puede recolectar remotamente información de configuración muy detallada acerca de los dispositivos. Está diseñado para ser un protocolo eficiente y con poco desperdicio de datos, de tal forma que no consuma el preciado ancho de banda y, por

tanto, haga lenta a toda la línea de productos de Cisco. Debido a que el CDP es propietario, es capaz de recolectar una gran cantidad de información utilizando una muy pequeña cantidad de datos inútiles. Existen otras herramientas para descubrir dispositivos "conectados localmente". Las herramientas de administración de la red SNMP son formidables para la administración centralizada, pero recolectan información menos específica acerca de la configuración de lo que puede hacer el CDP en los dispositivos de Cisco (el SNMP se estudia en el capítulo 13).

RECUPERACIÓN DE CONTRASEÑAS

A veces se presentan situaciones que hacen necesario recuperar la contraseña de un enrutador. Dos de las situaciones más comunes son:

- ▼ Se ha perdido una contraseña y no se puede encontrar ningún registro de ella.
- ▲ Se adquiere un enrutador usado y éste viene con contraseñas instaladas.

La recuperación de contraseñas requiere, como es natural, el ingreso al archivo de configuración del enrutador para encontrar la contraseña perdida, cambiarla o borrar el archivo de configuración completamente y reconfigurar el enrutador desde el principio.

El problema es que el archivo de configuración reside dentro del Privileged EXEC (modo de habilitación) del IOS, que en sí está protegido con contraseña. Por esa razón, la recuperación de una contraseña requiere el acceso a la versión no configurada del software IOS. Esta es la razón por la que también se requieren los procedimientos para la recuperación de la contraseña.

Existen varios procedimientos para la recuperación de contraseñas en los enrutadores de Cisco si se perdió una contraseña Line o Enable, y dependiendo del modelo del hardware de enrutador y la versión del software del IOS. Todos los procedimientos incluyen el restablecimiento de parámetros que le indican al enrutador cómo arrancar. Los enrutadores más antiguos de Cisco utilizan pequeños jumpers físicos, por lo que es necesario que abra la tapa del enrutador y restablezca los parámetros necesarios. Los enrutadores nuevos de Cisco cuentan con "jumpers por software" llamados *registros de configuración*, donde pueden modificarse las configuraciones. Un ejemplo de un parámetro en el registro de configuración es 0x2102. Los primeros cuatro bits (0-3) son los que indican el modo de arranque:

- ▼ Cuando los cuatro bits son 0000 (0), indican que el enrutador va a ingresar al modo rommon>> una vez que arranque.
- ■ Cuando los cuatro bits son 0001 (1), significa que el enrutador arrancará del sistema IOS almacenado en la ROM.
- ▲ Cuando los cuatro bits son de 0010 (2) a 1111 (F), significa que el enrutador consultará el archivo de configuración en el NVRAM para encontrar desde qué imagen del sistema IOS arrancar.

Recuperación de las Enable Passwords

Se utilizan dos procedimientos para recuperar Enable Passwords (Enable y Enable Secret). La que se use dependerá del modelo del enrutador, y a veces de la CPU o la versión de soft-

ware del IOS con la que está trabajando el enrutador. Si no encuentra aquí lo que necesita, una búsqueda rápida del término "password recovery" en el sitio Web de Cisco será de gran ayuda para encontrar un procedimiento específico.

Para recuperar una contraseña, debe llegar a la indicación rommom>> para recuperar contraseñas Enable o Enable Secret y la indicación test-system>> para recuperar una contraseña Line. Lo anterior se hace enviando una señal Break desde la terminal de la consola hacia el enrutador para interrumpir el proceso normal de arranque.

NOTA Es posible que el enrutador no responda a la señal Break que se envía desde los emuladores de terminal de PC. Debe saber la manera en que el emulador de terminal que está utilizando genera las señales Break. En algunos emuladores, el Break se genera con la combinación ALT+B; en otros, CTRL+B. Consulte la documentación de la ayuda de su emulador si llega a tener problemas para interrumpir el proceso de arranque del enrutador con Break.

Obtención del indicador de comandos rommon>

En el caso de cualquiera de los dos procedimientos para recuperar contraseñas Enable/Enable Secret, la primera parte (la obtención de la indicación rommon> del IOS) es la misma:

1. Conecte una terminal o una PC que ejecute software de emulación de terminal, al puerto de la consola del enrutador utilizando estos parámetros:
   - Velocidad de 9600 bauds (9600 baud rate).
   - Sin paridad (No parity).
   - 1 bit de detención (1 stop bit).
   - Sin control de flujo (No flow control).
2. Vaya a >prompt y teclee el comando **show version**. (Recuerde, perdió la contraseña Enable o Enable Secret, que sólo le quita el acceso a enable mode, pero no lo saca totalmente del IOS.)

```
TN3270 Emulation software.

2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
128K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)

Configuration register is 0x2102
```

3. La última línea del desplegado **show version** es el registro de configuración. El valor predeterminado de la fábrica suele ser 0x2102; y a veces 0x102. Escriba los parámetros en su enrutador para usos posteriores.
4. Reinicie el enrutador apagando y encendiendo la alimentación eléctrica.

5. Presione la tecla Break en la terminal (o la combinación de teclas que se requieren para enviar Break desde su emulador de terminal) durante los 60 segundos posteriores al encendido el enrutador.
6. Debe aparecer el indicador de comandos rommon>prompt (sin mostrar el nombre del enrutador).

Ahora que ha llegado a la indicación rommon>prompt, la mitad de la batalla para recuperar la contraseña está ganada. De aquí en adelante, el modelo del enrutador determinará lo que necesitará hacer para recuperar la contraseña (en algunos casos, la versión del IOS y la CPU también tienen que ver). A partir de aquí, hay dos caminos que se pueden seguir para la recuperación de la contraseña. De nuevo, consulte el modelo de su enrutador en la página www.cisco.com. Le informará cuál procedimiento utiliza su modelo. Con mucha frecuencia, tendrá que seguir el procedimiento 2 que se muestra más adelante.

Procedimiento 1 para la recuperación de la contraseña Enable Si el modelo de su enrutador requiere que siga el procedimiento 1 para la recuperación de la contraseña, siga estos pasos:

1. Teclee **o/r 0x2142**, y después presione Enter cuando aparezca >prompt. Esto cargará desde la memoria flash sin cargar el archivo de configuración del enrutador.
2. Teclee **i** cuando aparezca la indicación y después presione ENTER.
3. Se le hará una serie de preguntas sobre la configuración. Responda **no** a cada pregunta o presione CTRL-C para saltar toda esta secuencia.
4. Cuando aparezca Router>prompt, teclee **enable**.
5. Teclee **configure memory** o **copy starup-config running-config**. Esto copia el NVRAM en la memoria.
6. Teclee **write terminal** o **show running-config**. Estos comandos muestran la configuración del enrutador. Esto mostrará que todas las interfaces están deshabilitadas en este momento. Además, verá las contraseñas, tanto codificadas como no codificadas. Las contraseñas sin codificación pueden reutilizarse mientras que las codificadas deberán cambiarse por una nueva contraseña.
7. Teclee **configure terminal** y haga el cambio que quiera. Ahora, el indicador de comandos será **hostname(config)#**.
8. Para cambiar una contraseña dada, teclee **enable secret <password>** para cambiar la contraseña enable secret, por ejemplo.
9. Teclee el comando **no shutdown** en cada interfaz.
10. Teclee **config-register** 0x2102 (o el valor que haya escrito en el paso 2).
11. Presione Ctrl-Z o End para salir del modo configuración. Deberá aparecer **hostname#**.
12. Teclee **write memory** o copie **running-config startup-config** para guardar los cambios.
13. Teclee Reload para reiniciar el enrutador con el software del IOS de Cisco para arrancar desde la memoria flash.

Procedimiento 2 para la recuperación de la contraseña Enable Utilice este procedimiento en los enrutadores que deban utilizar el procedimiento 2 para la recuperación de la contraseña.

1. Teclee el comando **confreg 0x2142** cuando aparezca la indicación rommon>prompt. (Observe que **confreg** no es un error de dedo de **config**. Quiere decir registro de configuración, configuration register.) Cuando aparezca la leyenda "Do you wish to change configuration?" (¿Desea cambiar la configuración?), responda sí.
2. Teclee **reset** cuando aparezca rommon 2> prompt. El enrutador volverá a arrancar, pero ignorará la configuración almacenada.
3. Aparecerán varias preguntas acerca de la configuración. Teclee **no** en cada una de ellas. Opcionalmente, puede teclear Ctrl-C con el fin de evitar la secuencia inicial de configuración.
4. Teclee **enable** en la indicación Router> prompt. Esto lo ubicará en el modo enable (enable mode), y verá el indicador de comandos Router# prompt.
5. Teclee **configure memory** o copie **startup-config running config**. Esto copia la RAM no volátil en la memoria.
6. Teclee **write terminal** o **show running-config**. Estos comandos despliegan la configuración del enrutador y mostrarán que todas las interfaces se encuentran apagadas en ese momento. Además, podrá ver las contraseñas, ya sea codificadas o sin codificar. Las que no tienen codificación pueden reutilizarse; las codificadas deberán cambiarse por una nueva contraseña.
7. Teclee **configure terminal** y ejecute cualquier cambio que desee. Ahora aparecerá **hostname(config)#**.
8. Para modificar una contraseña dada, teclee **enable secret<password>** para modificar la contraseña enable (secret enable, por ejemplo).
9. En cada interfaz, teclee el comando **no shutdown**.
10. Teclee **config-register** 0x2102 (o cualquiera que haya sido el valor de registro de configuración anterior).
11. Presione Ctrl-Z o End para salir del modo de configuración. La indicación deberá ser host**name#**.
12. Teclee **write memory** o copie **running-config startup-config** para guardar sus cambios.
13. Teclee **Reload** para reiniciar el enrutador con el software del IOS de Cisco para arrancar desde la memoria flash.

Recuperación de la contraseña de línea

Debe forzarse al enrutador para iniciar en el modo de fábrica de diagnóstico para recuperar la contraseña de línea (Line) perdida. Consulte la publicación de instalación/mantenimiento del hardware del enrutador para obtener información específica acerca de la configura-

ción en modo de diagnóstico de fábrica del registro de configuración del procesador. En la tabla 4-5 se muestran los parámetros de hardware y software que necesitan los diferentes productos para arrancar en el modo de diagnóstico de fábrica.

Una vez que el enrutador ha sido puesto en el modo de diagnóstico de fábrica, siga estos pasos:

1. Teclee **yes** cuando se le pregunte si desea configurar las direcciones del fabricante. Aparecerá el indicador de comandos test-system>.
2. Teclee el comando enable para obtener el indicador test-system> enable.
3. Teclee config term y después show startup-config. Deberá ver en este momento el archivo de configuración del sistema. Encuentre la contraseña y escríbala. No intente cambiarla.
4. Reinicie el enrutador.
5. Utilice la contraseña de línea que recuperó (la que escribió) para registrarse en el enrutador.

Recuperación de contraseñas de enrutadores Cisco anteriores

Para recuperar contraseñas de enrutadores tradicionales de Cisco, es necesario cambiar los parámetros del registro de configuración utilizando un pequeño conector de hardware. Estos procedimientos no se estudian aquí. Consulte el sitio www.cisco.com para encontrar los procedimientos y recuperar contraseñas para los productos convencionales que se muestran en la tabla 4-6.

Procedimiento de recuperación	Plataformas que utilizan el procedimiento
Cambie el valor 0x8000 para arrancar en el modo de diagnóstico de fábrica. Utilice el comando **reload** para reiniciar; después cambie los parámetros de configuración de nuevo a 0x2102 cuando haya terminado.	Cisco AS5100, AS5200, AS5300 Cisco Series 1600, Series 2500, Series 3000 y Series 3600 de Cisco.
Coloque el pequeño conector en el bit 15 del registro de configuración; reinicie; y restablezca el pequeño conector cuando haya terminado.	Productos modulares.

Tabla 4-5. Parámetros del registro de configuración para ingresar al modo de diagnóstico de fábrica.

Procedimiento de recuperación	Plataformas heredadas de Cisco que utilizan los procedimientos
Técnica 3	Enrutadores IG que ejecutan software anterior al IOS 9.1 de Cisco.
Técnica 4	CGS, MGS, AGS, AGS+ y cualquier serie 70×0 de Cisco que ejecuta ROM anteriores al IOS 10.0 de Cisco.
Técnica 5	Servidores de comunicaciones 500-CS.
Técnica 6	1020 de Cisco.
Uso de las aplicaciones para ayudar a configurar enrutadores	

Tabla 4-6. Procedimientos para la recuperación de contraseñas para protocolos de enrutadores heredados de Cisco.

UTILIZACIÓN DE APLICACIONES PARA AYUDAR A CONFIGURAR ENRUTADORES

Hasta el momento en este capítulo se ha estudiado la configuración de enrutadores de manera manual. Cisco tiene implementada una herramienta de configuración en cada uno de sus enrutadores. La versión más actual de esta herramienta es su Security Device Manager (SDM, Administrador de Dispositivos de Seguridad). Es una GUI basada en Web que ayuda a simplificar la configuración y el uso de los enrutadores. Los diferentes modelos de enrutadores pueden contar con diversas herramientas para configuración integradas, pero proporcionan la misma funcionalidad básica. Regrese al capítulo 3 para obtener más información acerca de la configuración de enrutadores utilizando HTTP Server User Interfaz (interfaz de usuario de servidor HTTP).

Además de la herramienta de configuración incrustada, Cisco fabrica dos aplicaciones de software que sirven como herramientas:

- ▼ **ConfigMaker** Es una herramienta de rango intermedio que funciona con Windows. Se utiliza para configurar LAN Ethernet, además de conectividad WAN, y está diseñada para ser utilizada por administradores y consultores de red que tengan una experiencia razonable.
- ▲ **Fast Step** Es una herramienta más antigua que funciona con Windows. Se utiliza para configurar e instalar pequeños enrutadores y servidores de acceso de Cisco y está diseñada para que la utilicen usuarios menos sofisticados.

Vamos a revisar rápidamente la configuración de un enrutador utilizando cada herramienta. Para esto, revisaremos algunos conceptos acerca de la configuración de enrutadores que no se estudiaron durante el procedimiento de configuración.

Ambas herramientas utilizan una interfaz gráfica de usuario para ayudar en la tarea de poner en marcha los enrutadores. Ninguna de ellas trata de resolver grandes y complejos problemas de interconectividad. Un producto independiente llamado NetSys Baseliner se utiliza para el modelado y la administración de interconexiones empresariales. ConfigMaker y el Fast Step están diseñados para que los utilicen principiantes y personal de nivel intermedio.

ConfigMaker

ConfigMaker es una herramienta de Microsoft basada en Windows utilizada para diseñar y configurar pequeñas redes. Trabaja en configuraciones LAN y en conectividad WAN, con soporte de una amplia gama de dispositivos y protocolos de Cisco. ConfigMaker proporciona un entorno de trabajo de escritorio limpio e intuitivo que establece un buen balance entre la facilidad de uso y la funcionalidad. Pero no está diseñada para usuarios que demanden mucho poder de procesamiento, porque no cuenta con soporte para dispositivos del extremo alto, como los enrutadores de la serie 7000 de Cisco o los conmutadores de extremo alto. Ni tampoco soporta el protocolo LAN Token Ring ni cualquier enrutador que utilice una versión del IOS anterior a la 11.2.

ConfigMaker se ejecuta con Windows 98, Windows Me, Windows 2000, Windows XP o Windows NT 4.0 con al menos el Service Pack 3. Cisco lo proporciona sin ningún costo. Para probarlo, descargue una copia del sitio Web de Cisco www.cisco.com/public/sw-center/sw-netmgmt.shtml.

Para el creciente número de personal técnico en compañías pequeñas y medianas que desee administrar sus propias configuraciones de red, ConfigMaker es quizás la solución (siempre y cuando sus redes estén construidas parcial o totalmente con productos Cisco).

El entorno de escritorio del ConfigMaker

En el centro del escritorio del ConfigMaker se encuentra un área para el diagrama de la red en que se colocan los "objetos" de la red, se configuran y conectan. Al principio, el área para el diagrama de la red está vacía, como una hoja de papel antes de que se dibuje la primera línea. El área para el diagrama de la red está rodeada por tres ventanas; cada una de ellas le ayuda a construir una red hasta que la termine.

- ▼ **Ventana Device (Dispositivo)** Es una fuente de dispositivos que pueden ponerse en el Network Diagram; se localiza en el panel superior izquierdo.
- ■ **Ventana Connections (Conexiones)** Es una fuente de conexiones de área amplia para colocarlas sobre el Network Diagram; se ubica en el panel inferior izquierdo.
- ▲ **ConfigMaker de Cisco** Es una lista de verificación de las etapas cronológicas que deben terminarse durante la configuración de una red. Se localiza en el panel que está en el extremo derecho.

El primer paso consiste en arrastrar los dispositivos desde la ventana Device hasta el área del Network Diagram. Es una proposición muy simple; sólo seleccione los dispositivos que van a formar parte de la red: enrutadores, concentradores, cables de LAN, etcétera. Conforme cada dispositivo se coloca sobre el diagrama, el ConfigMaker solicita los parámetros necesarios para que el dispositivo funcione. Las rutinas del indicador son similares a la rutina Agregar nuevo hardware del panel de control de Windows de Microsoft.

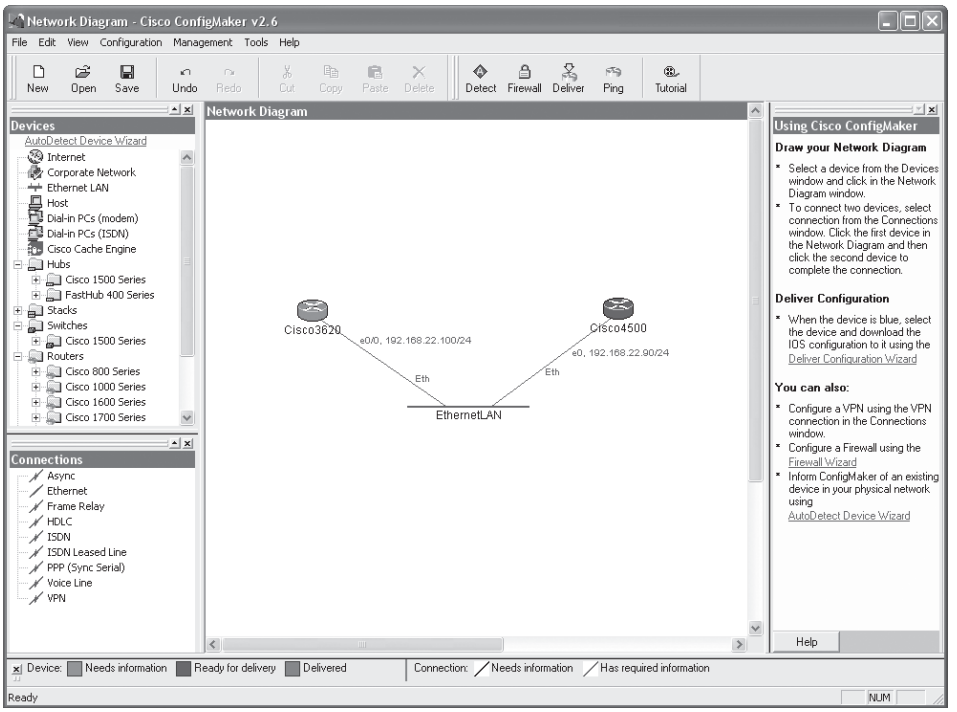


Figura 4-9. Apariencia del escritorio de ConfigMaker.

Una vez que los dispositivos se han colocado en el diagrama, es hora de conectarlos a la red. Esto se hace arrastrando una o más conexiones en el diagrama desde la ventana Connections. Para conectar un dispositivo a la red, en primera instancia, seleccione una conexión y después el dispositivo a conectar. En la figura 4-9 se despliega el escritorio de ConfigMaker, que muestra los comienzos de una red Ethernet desplegados en el área del diagrama de la red, donde dos enrutadores Cisco se encuentran conectados a una LAN Ethernet. El usuario puede seguir agregando dispositivos y conexiones hasta que toda la red aparezca en el diagrama.

Metodología del ConfigMaker

La construcción de una red mediante esta interfaz gráfica es muy útil para conceptualizar la topología de la red, pero ConfigMaker es más que un programa para hacer diagramas de redes. Cada dispositivo que se coloca en el diagrama dibujado en la ventana Device, posee cierto grado de inteligencia. Conforme se van agregando objetos a la red (dispositivos o conexiones de red), ConfigMaker solicita detalles relativos a ese artículo, como parámetros, nombres, etcétera. Esta información se almacena en una base de datos escondida debajo del diagrama y ConfigMaker la utiliza para verificar que todo sea consistente y esté completo.

ConfigMaker obliga a que exista una metodología para el aseguramiento de la calidad respecto al proceso de diseño de la red, como se describe a continuación:

- Conforme se agregan dispositivos, se recolecta información sobre ellos.
- Se verifica la consistencia de la información con el resto en la base de datos.
- Si se presentara un error, ConfigMaker le indica al usuario que lo corrija de inmediato.
- La lógica basada en reglas del ConfigMaker sigue verificando que toda la red esté correcta conforme se agregan nuevos objetos (dispositivos o conexiones).

NOTA Como principiante perceptivo que es usted, quizás se esté preguntando por qué Ethernet está en las ventanas Devices y Connections. Si selecciona el icono Ethernet de la ventana Devices, éste se encuentra definido para su diagrama como un segmento de red de área local; arrastre Ethernet de la ventana Connections, y se convertirá en un enlace a una red de área amplia. En otras palabras, el segmento LAN de Ethernet (un cable o un gabinete de concentrador) es tratado como un dispositivo físico, mientras que la conexión lógica de Ethernet representa una vinculación de interconexión.

Para ver la base de datos que el ConfigMaker conserva, haga clic con el botón derecho sobre cualquier dispositivo y seleccione **Properties**. Aparecerá un cuadro de diálogo con varias fichas, presentando toda la información conocida acerca del dispositivo. En la figura 4-10, por ejemplo, se muestra la ficha Hardware Configuration (Configuración de hardware). La ventana que se encuentra a la izquierda de la ficha contiene todos los módulos posibles que

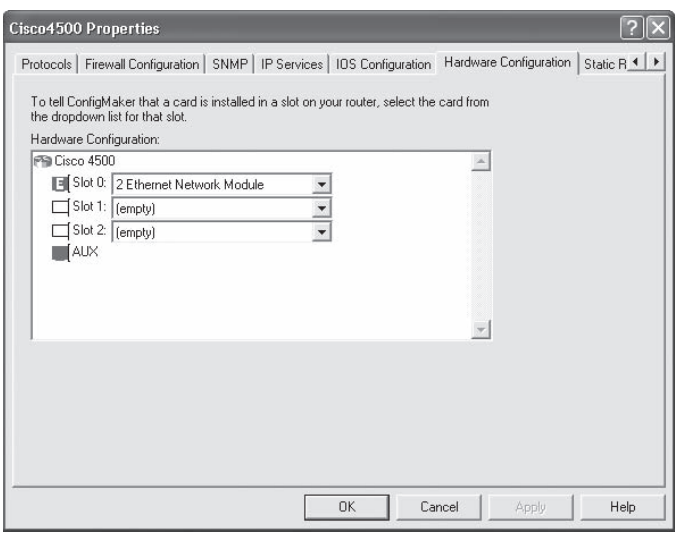


Figura 4-10. Un vistazo al cuadro de diálogo Properties del ConfigMaker de una enrutador 4500 de Cisco.

pueden conectarse al dispositivo. La ventana de la derecha muestra la configuración actual. En este ejemplo, el 4500 de Cisco está configurado con un módulo de seis ranuras de Ethernet y un módulo de un puerto T1/ISDN. ConfigMaker cuenta con la lógica para identificar casi todos los errores de configuración antes de que sucedan: se evita que el usuario inserte un módulo de red en un dispositivo incompatible, y cada dispositivo debe tener la interfaz adecuada antes de que éste pueda conectarse a la red. Echándole un vistazo a las figuras 4-9 y 4-10, observará que al enrutador 4500 de Cisco se le permitió conectarse a la red Ethernet porque se configuró primero con su interfaz Ethernet de seis puertos y también pudo enlazarse a una conexión T1/ISDN.

Los cuadros en la parte inferior de la pantalla de ConfigMaker (figura 4-10) forman una leyenda con las condiciones del estado, con teclas a colores. En la tabla 4-7 se proporciona la leyenda correspondiente a cada color. Un icono o línea de conexión de dispositivo cambiará los colores en la pantalla, a medida que varíe el estado de la configuración del objeto.

Construcción de una red con ConfigMaker

El panel Using Cisco ConfigMaker (Uso de Cisco CofigMaker) es un sistema de ayuda y una lista de verificación en uno. Se ubica a la derecha del Network Diagram y utiliza asistentes para guiar al usuario por las diferentes etapas del proceso de la configuración de redes. El panel Using Cisco ConfigMaker se divide en tres partes, dos de las cuales tienen asistentes dedicados a un trabajo en particular:

- **AutoDetect Device Wizard (Asistente para autodetección de dispositivo AutoDetect)** Es una serie de cuadros de diálogo para agregar nuevo hardware que reúnen la información necesaria acerca de la descripción y los parámetros de los dispositivos de red.
- **Deliver Configurations Wizard (Asistente para configuraciones de entrega)** Sirve para descargar automáticamente archivos config a los dispositivos.

Color	Estado de la configuración
Gris	Se necesita información adicional acerca del dispositivo o la conexión.
Negro	Se necesitan direcciones (direcciones IP, submáscaras, etcétera) para el dispositivo.
Azul	El archivo config del dispositivo está listo para entrega (o la conexión cuenta con la información que se requiere).
Rojo	El archivo config del dispositivo fue entregado y se encontró un error.
Verde	El archivo config del dispositivo se entregó con éxito.

Tabla 4-7. Claves de color que registran el estado de la configuración.

- **Firewall Wizard (Asistente para firewall)** Le permite establecer directivas en un firewall y determinar las LAN que pueden acceder a Internet o a una red corporativa, además de las LAN internas que pueden acceder entre sí.

AutoDetect Device Wizard El uso de este asistente es opcional. Si recurre a él, automáticamente ubicará e identificará el tipo de hardware que se va a configurar. El dispositivo AutoDetect es de gran ayuda si va a reconfigurar dispositivos de manera remota y no están ahí para inspeccionar físicamente los componentes de hardware y ver los números de modelo, módulos de interfaz instalados, etcétera. El AutoDetect Device Wizard soporta conexiones de red y de terminal virtual hacia los dispositivos que se están configurando.

Firewall Wizard (Asistente para firewall) Se utiliza para configurar y definir las directivas del firewall. Es decir, es un mecanismo que puede utilizar para decidir cuáles LAN pueden acceder a Internet y, dentro de la red, cuáles LAN pueden acceder entre sí. Es una herramienta útil porque le permite establecer directivas para cada LAN de su red. En la figura 4-11 se muestra la pantalla del Firewall Wizard, donde puede fijar y administrar directivas para el firewall.

Deliver Configurations Wizard (Asistente para configuraciones de entrega) Este asistente hace precisamente eso: descarga automáticamente archivos config que se generaron en el ConfigMaker en los dispositivos objeto destino. Para utilizar este asistente, los dispositivos deben estar conectados (por medio del puerto de la consola o del puerto de red) a la PC en que está trabajando con ConfigMaker.

Análisis del producto ConfigMaker

Un beneficio importante del ConfigMaker es que los usuarios podrán observar que es difícil cometer errores. Muchos errores de configuración tienen que ver con malas elecciones para

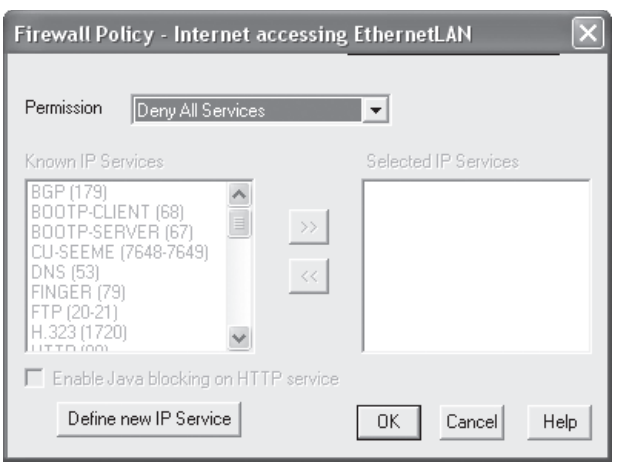


Figura 4-11. El Firewall Wizard se utiliza para configurar firewalls en el ConfigMaker.

dispositivos determinados. En el ConfigMaker (que es específico para Cisco), si trata de poner un dispositivo incompatible en un enrutador, un mensaje de error lo detendrá. Si se le olvida hacer una acción que debe realizarse, ConfigMaker se lo indicará. Esta capacidad para asegurar la calidad no sólo ayuda a evitar errores, sino también a mantener al usuario actualizado acerca de las opciones del producto (las que cambian constantemente).

Quizá el beneficio más importante del ConfigMaker es que no necesita conocer la interfaz de línea de comandos del software IOS de Cisco para configurar los dispositivos y conexiones de red. Cuando necesite ingresar algo, las opciones correctas se encuentran frente a usted. La GUI basada en Windows hace esto posible. El uso de las convenciones de Windows (la indicación Agregar nuevo hardware, la barra de menús, etcétera) y las claves de color lo hace fácil de usar y de aprender.

ConfigMaker proporciona un balance lo suficientemente bueno entre capacidad y facilidad de uso como para que los principiantes y quienes tienen experiencia en conectividad pueden usarlo. Es como un regalo mandado por Dios para los principiantes, no sólo para que una red trabaje correctamente, sino para aprender los fundamentos de la interconectividad.

Sin embargo, ConfigMaker tiene límites. No está fabricado para el diseño y administración de redes grandes y complejas. Por ejemplo, el sistema sólo soporta enrutadores hasta la Serie 4000 de Cisco y no la serie de enrutadores de extremo superior, y su limitada funcionalidad no le permitirá simular el comportamiento de una red.

Fast Step

Fast Step de Cisco es una utilería de configuración que se incluye con los enrutadores de extremo inferior y con los servidores de acceso. Está diseñado para que lo use el usuario de la red que está iniciándose en este campo, para configurar conexiones de extremo a extremo entre una PC y un proveedor del servicio de Internet (ISP) o intranets corporativas. Fast Step funciona con los sistemas operativos Windows 95, 98, NT 4.0, 2000 o XP. Viene en un CD-ROM para su instalación en una PC de Windows, y puede utilizarse de dos maneras:

- ▼ Para configurar el enrutador interactivamente mientras está conectado a él, ya sea a través de un cable serial desde el puerto COM de la PC hasta el puerto de consola del enrutador, o por medio de un enlace Ethernet.
- ▲ Para construir un archivo de configuración para descargarlo después al enrutador o como base para configurar otros enrutadores (el archivo puede leerse por medio del Setup Wizard [Asistente para configuración] del Fast Step).

Después de la instalación del Fast Step, si hace clic en el icono, éste comienza una secuencia de cuadros de diálogo que invitan al usuario a ingresar la información necesaria para configurar e instalar el enrutador. La secuencia puede incluir hasta una docena de cuadros de diálogo, en función de las opciones que se tomen. Como ayuda para arreglar las cosas, cada pantalla de Fast Step tiene una ventana Tasks (Tareas) en el lado izquierdo. Verá dónde se encuentra durante el proceso si busca la tarea que está resaltada en la ventana Tasks, en el lado izquierdo de cualquier ventana de Fast Step. Como se expresó en la tabla 4-8, Fast Step agrupa a las tareas de configuración en cuatro pasos principales.

Búsqueda y conexión

Fast Step comienza pidiendo información general acerca de la sesión de configuración, como el modelo del enrutador que se va a configurar y si se va a crear un nuevo archivo config o se va a utilizar un archivo preconfigurado.

Etapa	Descripción de tareas
Búsqueda y conexión	Proporcione el número de enrutador; seleccione el modo de configuración (interactivo o descarga); defina el tipo de conexión (ISP o corporativa); proporcione los parámetros; dirección IP y números telefónicos del proveedor del acceso, nombre de usuario, contraseña, etcétera.
Seguridad	Especifique el nombre del enrutador; contraseña de sólo lectura del enrutador; y contraseña Enable Secret del enrutador; especifique los tipos de servicios (servidor Web, servidor de correo, servidor FTP).
Direccionamiento local	Especifique la dirección IP de la conexión LAN proporcionada por el ISP o intranet corporativa.
Configuración y prueba	Guarde el archivo config en el enrutador y ejecútelo; guarde el archivo config para utilizarlo con otros enrutadores.

Tabla 4-8. Las cuatro partes de las tareas de configuración del Fast Step.

Después le solicitará información más específica. Fast Step le solicita que ingrese el nombre de usuario de PPP (Protocolo Punto a Punto, Point- to-Point Protocol) que le proporcionó su ISP o su administrador de la intranet corporativa. El nombre de usuario del PPP es sensible a las minúsculas y mayúsculas, por lo que debe asegurarse de teclearlo exactamente como aparece en la información que le proporcionó su ISP o su administrador de red.

A continuación ingrese su contraseña PPP, que no es su contraseña de acceso a la red. La contraseña PPP es sólo para el acceso remoto de marcado telefónico a través de una conexión de enrutador a enrutador. Asegúrese de que la contraseña cumpla con los requisitos de su ISP o red corporativa (número mínimo de caracteres, etcétera). Esta contraseña se conoce con el nombre de contraseña "PAP" o "CHAP" y sí importa si se escribe con mayúsculas o minúsculas. Por último, ingrese al enrutador central o nombre PPP del enrutador al que se va a conectar (no el nombre del enrutador que está configurando). PPP, CHAP y PAP se estudian en el capítulo 6.

La segunda mitad de la etapa de búsqueda y conexión consiste en proporcionar la información y los parámetros necesarios para conectar el enrutador a Internet. Para lo anterior, Fast Step le indica más parámetros como el tipo de conmutador, SPID de ISDN y números telefónicos de acceso (SPID quiere decir ID del Proveedor de Acceso, service provider ID, generalmente un ISP).

Después, las cosas interactúan entre sí, al menos para los estándares de un principiante. En la figura 4-12 se muestra Fast Step pidiendo información acerca de las direcciones IP.

Sólo se puede tomar una de tres opciones:

- ▼ No proporcionar ninguna dirección porque no tiene ninguna todavía.
- ■ Dar un rango de direcciones que le proporcionará su ISP o su administrador de la red corporativa.
- ▲ Proporcionar una dirección de red IP y una máscara de subred.

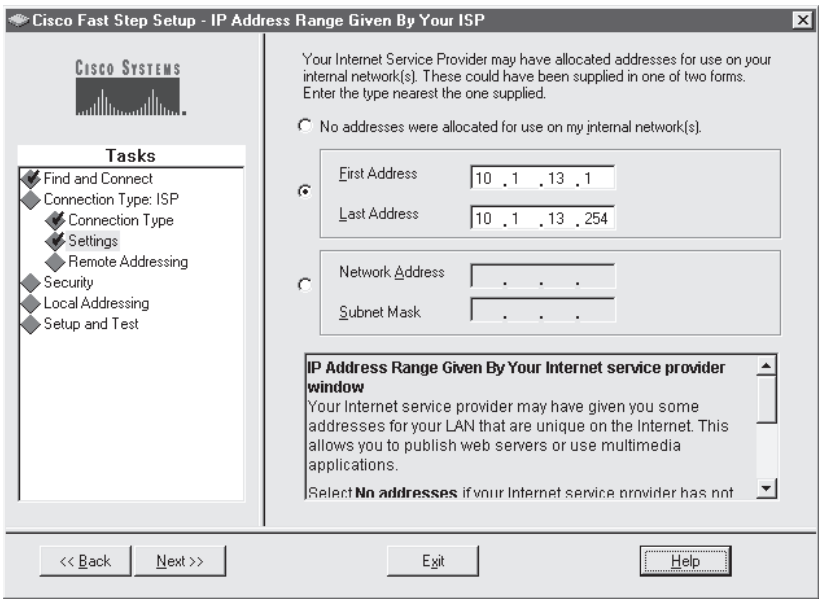


Figura 4-12. Fast Step le solicitará información acerca de la dirección IP.

Esta información es para identificar el segmento LAN al que el usuario se conectará con la dirección única a Internet. Fast Step necesita esta información para hacer la conexión. Estos parámetros son, en esencia, la dirección del usuario en la forma como se presenta al resto de Internet (o la comunidad de la intranet corporativa). Fast Step puede descubrir la dirección automáticamente pero permite que el usuario la ingrese, si así lo desea.

Seguridad

A continuación Fast Step solicita los parámetros que tengan que ver con la seguridad del enrutador y con la publicación del servidor del enrutador. En la figura 4-13 se muestra la solicitud que le hace el sistema a un usuario para asignar un nombre al enrutador, una contraseña de sólo lectura y una contraseña enable.

Aquí se aplica gran cantidad de reglas a los nombres y contraseñas (si se viola una regla, un mensaje de error lo detendrá). El sistema de ayuda en línea indica al usuario cuáles son las reglas. Estas contraseñas se aplican para tener acceso al enrutador en sí, con fines administrativos. Luego, Fast Step le permite al usuario configurar una o varias de estas cuatro opciones de servicios de Internet:

- ▼ Único servidor (un servidor Web y un servidor de correo, la opción más común).
- ■ Servidor Web (una página Web sin servicio de correo electrónico).
- ■ Servidor de correo (solamente servicios de correo electrónico por Internet).
- ▲ Servidor FTP (la capacidad de que los usuarios de Internet descarguen información de su sitio).

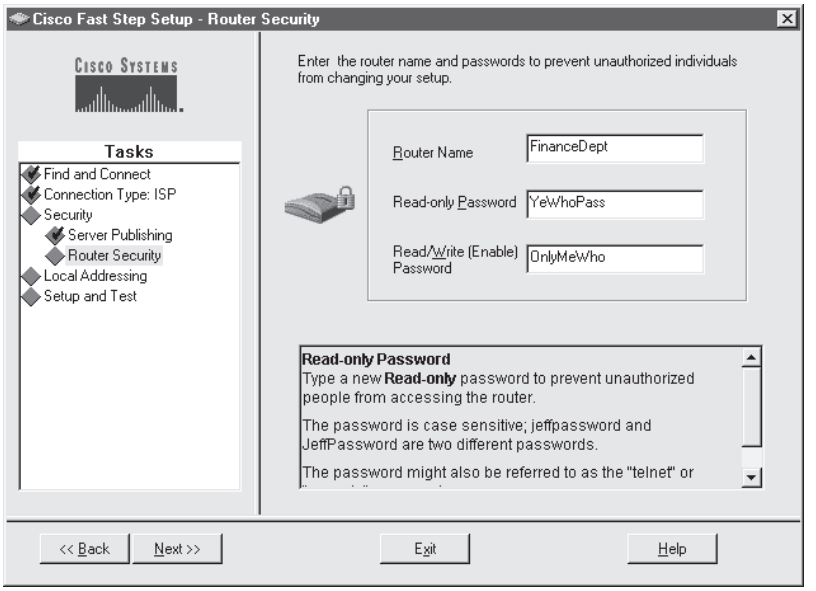


Figura 4-13. Fast Step solicita un nombre y contraseñas administrativas para el enrutador.

Los profesionales de la interconectividad a menudo les llaman a estas opciones "servidores". Por ejemplo, si el parámetro para proporcionar descargas FTP de la LAN del usuario se establece en "yes", esa LAN está trabajando un servidor FTP. No se desilusione por esto; es sólo un término gracioso para nombrar un servicio.

Direccionamiento local

Por último, Fast Step solicita direcciones IP de la red de área amplia a la que está conectada la LAN del usuario. Estas direcciones, que se muestran en la figura 4-14, identifican el ISP o la red corporativa en Internet.

Observando las figuras 4-12 y 4-14, notamos que Fast Step desea dos conjuntos de direcciones, que se utilizan para identificar los dos segmentos de red independientes que participarán en la conexión de la LAN remota del usuario a Internet. Lo anterior podría provocar confusión al principiante. Tenga presente que el enrutador se conectará al ISP, la Intranet, o ambos, por medio de una conexión de punto a punto, enrutador a enrutador (no a través de una nebulosa dirección IP de Internet). La información acerca de la dirección que se proporciona en la figura 4-13 se utiliza para identificar al enrutador que se está configurando mediante Fast Step. Este enrutador es lo que conecta a la LAN del usuario a Internet. Debido a que esa LAN tendrá más de un usuario operando en Internet en un momento dado, Fast Step solicita un rango de direcciones IP, una por usuario (figura 4-13). Por otra parte, la dirección remota solicitada en la figura 4-14 se utilizará para identificar el segmento de red que identifica al ISP o la intranet mediante la que se conectará el usuario.

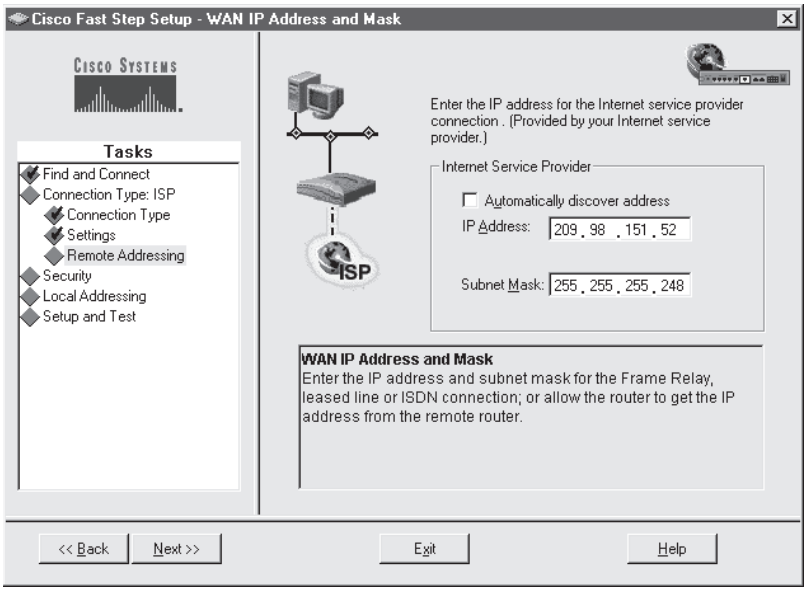


Figura 4-14. Fast Step le pedirá la información acerca de la dirección de los ISP.

La figura 4-15 sirve de ayuda en la clasificación de estas direcciones. Generalmente, a la LAN local hacia el usuario (y el enrutador que se está configurando con Fast Step) se le asigna un bloque de direcciones IP. El ejemplo de la figura 4-12 tiene un bloque de 254 direcciones que se asignaron para la red interna del usuario (de 10.1.13.1 a 10.1.13.254).

El ISP o la intranet corporativa cuenta con una dirección IP para identificar su segmento de red, y una submáscara de red para esa dirección IP (255.255.255.248) le permite tener hasta seis posibles direcciones anfitrión dentro de esa subred.

Si el escenario invita a conectarse a una intranet corporativa, un tercer segmento de red entra en juego: el de la red principal de la corporación, que está en el lado izquierdo de la figura 4-15. Para el usuario que está configurando el enrutador, la nube de conectividad, ubicada en medio de la figura, representa el mismo servicio si la conexión se realiza a través de una red privada corporativa o de un ISP, y tal vez sólo se pueda alcanzar al segmento de red corporativo del lado izquierdo a través de un firewall.

Configuración y prueba

En la última parte de la configuración, Fast Step le permite terminar el proceso de configuración del enrutador tomando algunas de las acciones siguientes:

- ▼ Cargar el archivo config en el enrutador.
- ▲ Hacer una copia por separado del archivo config.

Si el usuario opta por hacer una copia por separado, desde luego que se le debe asignar un nombre al archivo. Existe la opción de guardar el archivo tal como está en el formato

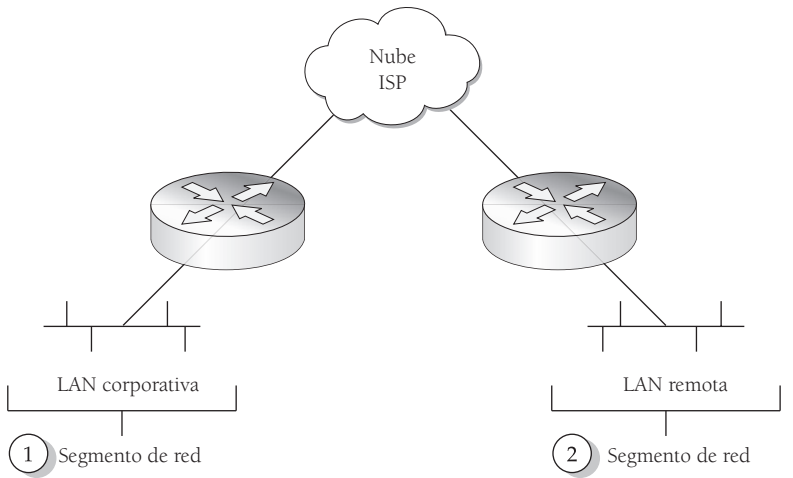


Figura 4-15. Existen tres segmentos de red en una conexión remota de intranet.

CFG del Fast Step para usarlo en otros enrutadores, o guardarlo con el formato de comando del IOS para su uso como una plantilla a partir de la cual construir archivos config ligeramente diferentes para otros enrutadores. A continuación se muestra la parte superior de un archivo config del enrutador 801 de Cisco, que se creó utilizando Fast Step:

```
! Cisco IOS router configuration file
! Automatically made by Cisco Fast Step v2.0
! Designed for Cisco C801
! March 31, 1999
! Cisco Fast Step Template

no service udp-small-servers
no service tcp-small-servers
service password-encryption
hostname veltepub003
username tonyv password Password
enable secret SuperSecret
no ip source-route
isdn switch-type basic-5ess
.
.
.
```

Análisis del producto Fast Step

La serie de cuadros de diálogo de Fast Step le piden al usuario que proporcione toda la información que se necesita para configurar una conexión de extremo a extremo entre una PC casera o de una oficina pequeña y un ISP (o una intranet corporativa). Esto es bueno porque, le guste o no, las configuraciones de red pueden convertirse en una tarea muy compleja.

Comparados con los del ConfigMaker, los indicadores dan más cabida a que se cometan omisiones u errores. Esto en gran medida se debe a que la tarea del Fast Step es diferente a la del ConfigMaker. Por ejemplo, para decidir cuál interfaz configurar en una ranura de un enrutador Cisco, el ConfigMaker le proporciona un ventana que sólo contiene interfaces compatibles con el enrutador que se está configurando. En contraste, Fast Step casi siempre solicita respuestas de extremo abierto que provienen de fuentes externas, en lugar de ofrecer una ventana de selección de entrada dentro de la pantalla de Fast Step. El usuario debe consultar documentos externos para elementos como números telefónicos, números de control, nombres de usuario, direcciones IP, etcétera. Cisco sabe esto y, por tanto, proporciona hojas de datos en su guía de introducción para ayudar a los usuarios a reunir los parámetros de configuración necesarios antes de comenzar.

En Fast Step existe una gran cantidad de opciones para editar los datos ingresados al sistema. Esto ayuda al usuario a identificar errores a medida que se van presentando. Si el usuario trata de ingresar algo ilegal, aparecerá en el lado derecho del campo un signo de exclamación, además de un mensaje de error en la ventana correspondiente. Esta edición puede ser una bendición o un dolor de cabeza. Por ejemplo, si trata de ingresar una contraseña PPP errónea, el cuadro de aviso le informa "does not meet the accepted rules" (no cumple con las reglas aceptadas). Pero, vaya, ¿cuáles *son* esas reglas? Presione el botón Ayuda, y la respuesta es "que la contraseña es una contraseña de acceso que su proveedor de servicio de Internet o administrador de red le proporcionó", cuando lo que en realidad necesita saber son las reglas de la sintaxis. El subsistema de ayuda Fast Help es bueno, en general, pero a veces no es muy claro.

Sin embargo, con la ayuda de las indicaciones y la diversidad de opciones con que cuenta Fast Step, así como con un poco de esfuerzo, un principiante puede configurar e instalar un enrutador de extremo inferior conectado a Internet. Sin la ayuda de Fast Step, una persona no especializada en este campo tendría muy pocas posibilidades de configurar y poner a trabajar un enrutador. Puede ser que la herramienta Fast Step no sea perfecta; sin embargo, le ofrece la posibilidad de dar batalla.

CAPÍTULO 5

Conmutadores

En los dos capítulos anteriores se estudiaron los enrutadores, que trabajan entre redes. Una interconexión es, por definición, una colección de redes de área local conectadas por medio de enrutadores. En otras palabras, un paquete que tenga que viajar por medio de uno o más enrutadores ha recorrido una interconexión. De un momento a otro, ese paquete llegará a la red de destino (punto de destino de la dirección IP).

¿Pero qué pasa entonces? En ese momento, el mensaje ha atravesado el último enrutador y debe ingeniárselas para encontrar un camino a su destino por el cableado de la red. En otras palabras, deberá dejar la nube de la interconexión y no deberá buscar otra interfaz de enrutador, sino el puerto de conexión específico en que está conectado el host de destino. Puesto que casi todas las PC y los servidores carecen de conexiones de red directas a un enrutador, existe todavía un tramo de camino por recorrer.

Así que los hosts no cuentan con sus propios puertos de enrutador. Bueno, los hosts (PC y servidores, por ejemplo) necesitan conectarse a las redes de alguna forma. El enrutador está diseñado para conectar redes a otras redes, por lo que éste es de poca utilidad cuando se trata de conectar hosts en forma física. Ahí es precisamente donde entran a escena los conmutadores, que brindan conectividad local a los hosts y son los ladrillos con que se están construidas las LAN.

La última parte del viaje de un mensaje se lleva a cabo dentro de un edificio o un campus con oficinas. Aquí se debe hacer una transición desde las líneas de telecomunicaciones de la nube de conectividad, pasando por el cable instalado a través de las paredes y techos del edificio, hasta la placa de contactos ubicada sobre la pared y, por último, hasta el dispositivo de host en sí. Esta última etapa requiere una transición a la dirección física del host de destino. A esta dirección se le llama dirección de control de acceso al medio (Media Access Control o MAC). La dirección IP lo lleva al vecindario, mientras que la dirección MAC lo lleva a la puerta principal de la casa. Las direcciones MAC deben ser siempre únicas e identifican la NIC (Network Interface Card, tarjeta de interfaz de red) que conecta el dispositivo de destino con su LAN. Estas direcciones sirven como una especie de número de serie de un determinado dispositivo físico, por lo que cualquier dispositivo instalado en cualquier red en el mundo puede ser identificado de manera única.

Pero un solo paso desde una dirección IP mundial hacia una dirección MAC individual de un host sería muy abrupto. Es necesario que exista un paso intermedio que separe el nivel del enrutador de alta velocidad del de las NIC de baja velocidad. En efecto, la carencia de una zona de almacenamiento significaría permitir el acceso de vehículos lentos en una carretera interestatal de alta velocidad. Aunque las NIC y los hosts fueran extraordinariamente rápidos, se necesitaría un nivel de procesamiento intermedio para administrar el sistema en forma correcta. Un conmutador proporciona ese paso intermedio. En la figura 5-1 se muestra el lugar donde se conecta este dispositivo.

En este capítulo, se analiza esa zona que reside entre el escritorio y el enrutador que lo enlaza a la LAN. Éste es el reino de los cables y los conectores. Nos damos cuenta que los ojos se comienzan a nublar cuando la plática toma el tema de los paneles de plantas y cubiertas de cables, como si todas estas cosas, por alguna razón, fueran más adecuadas para el conserje del edificio; pero el tema de la conectividad local no es tan mundano como piensa. A medida que el equipo de conectividad de alta tecnología se extiende desde la red troncal hasta el escritorio, la decisión de cómo conectar hosts individuales y grupos de trabajo se ha convertido en un aspecto estratégico para la conectividad empresarial. Los avances de la

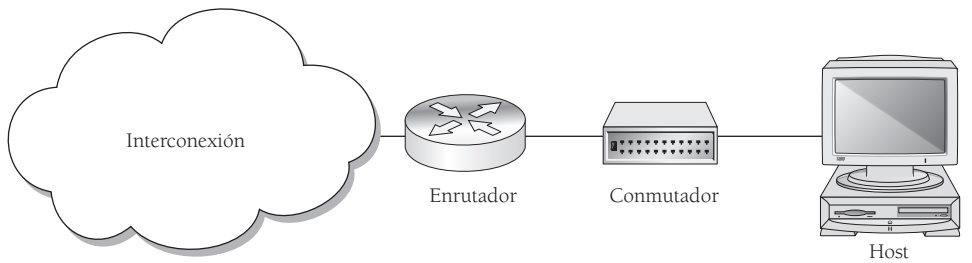


Figura 5-1. Los conmutadores se encuentran ubicados entre las espinas dorsales y los hosts.

tecnología están presentándose a pasos agigantados en el campo de la conectividad local. Por tanto, es importante que comprenda los fundamentos de este tema, incluidos algunos aspectos específicos del funcionamiento de los conmutadores de Cisco.

TOPOLOGÍAS DE LAS REDES

A la disposición física de una red se le conoce como *topología*. Hace como veinte años, no había muchas opciones (si es que las había) en cuanto al diseño de una topología de red.

Aunque había (y hay) muchas formas de hacerlo, vamos a estudiar una LAN típica de la "vieja escuela". Para construir una LAN, se instalaba un cable coaxial llamado *Thicknet* por todo su edificio y conectaba los hosts a dicho cable directamente. El cable Thicknet era la espina dorsal de la red. La conexión directa de los hosts a la espina dorsal traía como resultado la famosa topología en bus. Un *bus* es un cable (o una tarjeta de circuito impreso que funciona como cable) y una topología en bus era donde todos o casi todos los dispositivos de red se conectaban a un solo cable, que es como dirigir a todos a una calle sin salida en lugar de hacerlo por las calles laterales. En la figura 5-2 se muestran dos topologías típicas de red antiguas.

A medida que se desarrolló la tecnología de red, las topologías evolucionaron un poco con la introducción de servidores terminales, que hicieron posible conectar indirectamente terminales "tontas" a la LAN. Esto fue un punto positivo, porque brindó a los usuarios individuales acceso fácil a más de una minicomputadora o equipo mainframe. Otro avance fue la presentación de un tipo de cable coaxial más delgado llamado *Thinnet*, que era más barato y con el que se trabajaba mucho más fácil que con el cable Thicknet. Pero estas mejoras fueron sólo incrementales; la topología de red utilizada fue básicamente la topología en bus.

El problema con las topologías físicas en bus fue que si algo fallaba en el troncal, toda la red fallaba (o al menos una buena parte de ella). Otra desventaja era que la conexión de hosts significaba navegar por el techo falso, encontrar el cable troncal, hacer la conexión correspondiente, instalar un segundo cable desde la conexión hasta el dispositivo y, después, probar la conexión para ver si trabajaba. No sólo era más posible que fallaran las redes antiguas y resultaba más difícil instalarlas, sino que también el equipo era muy voluminoso y caro.

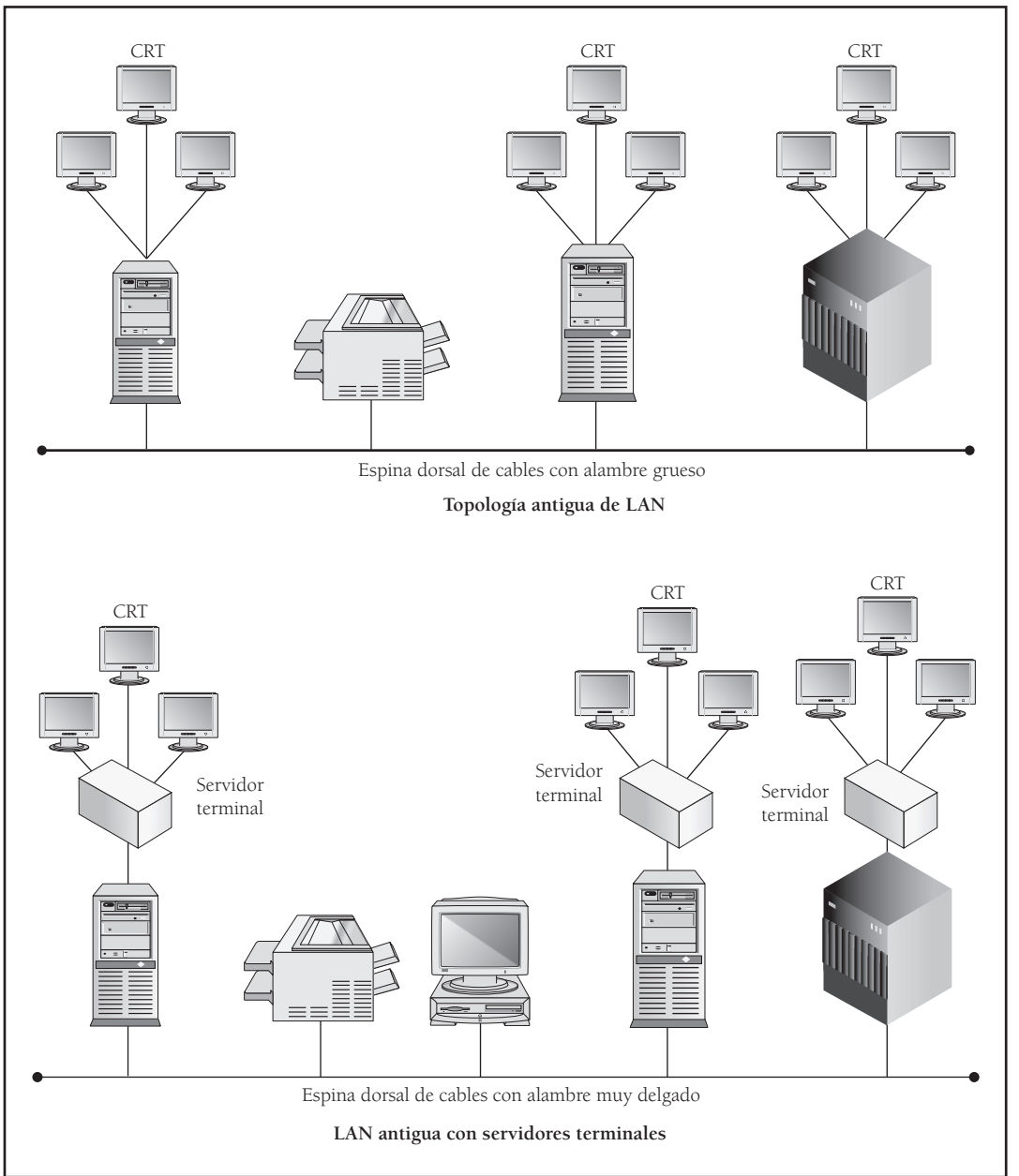


Figura 5-2. Las topologías antiguas de red empleaban conexiones con cables de alambre grueso y delgado.

Las cosas han cambiado significativamente desde entonces. En la actualidad, casi todos los hosts están conectados a las redes por medio de conmutadores, que proporcionan a los

administradores de red una gama más amplia de opciones para la selección de la topología física y lógica de las redes. Los conmutadores son modulares en el sentido de que pueden agregarse dispositivos y hosts sin tener que realizar modificación alguna en la espina dorsal de la red. Pero sobre todo, los conmutadores acaban con la necesidad de la topología física en bus, facilitando la instalación y administración de varias LAN. En la actualidad, los diseñadores de redes utilizan la topología en estrella en lugar de una LAN saturada.

NOTA El término "LAN" puede ser confuso. En tiempos pasados, una LAN era una troncal central instalada en un edificio a la que se le conectaban directamente todos los componentes de la red. En la actualidad, ese mismo edificio puede tener docenas de conmutadores que sirven como puntos de conexión a los hosts, con los conmutadores, a su vez, conectados a una espina dorsal. Cualquier medio de transmisión compartido de red es una LAN. Un conmutador es un medio compartido, al igual que el cable central que forma una espina dorsal. Aun los expertos utilizan el término "LAN" o "red de área local" para describir de manera informal una red local compuesta por varias LAN. Para evitar confusiones, en este libro utilizaremos el término "segmento LAN" para describir una medio compartido de red, que es el bloque de construcción básico de las topologías de red. Un segmento LAN está definido por un conmutador o cable. En estos días, el término "LAN" se refiere con frecuencia a una colección de segmentos LAN dentro de un edificio o campus.

Fragmentar las redes en LAN más pequeñas facilita la satisfacción de las necesidades actuales y todavía da oportunidad a modificaciones y crecimientos futuros. La segmentación de redes mejora el desempeño de la red aislando el tráfico. Es muy probable que los usuarios de un grupo de trabajo o un departamento se envíen mensajes entre sí, por lo que colocarlos en su propio segmento LAN significa que los demás no se verán afectados por el tráfico que se genere. La confiabilidad es mejor, porque lo que sucede en un segmento LAN no afecta a toda la red; la falla es aislada dentro del segmento donde inició ésta. Los administradores de red pueden identificar con mayor facilidad la ubicación de una falla debido a la presencia de puntos de transmisión entre los diferentes segmentos LAN (una característica importante en redes más complejas). Asimismo, la modularidad de las redes jerárquicas mejora su seguridad y administración, porque los dispositivos pueden agruparse de forma tal que satisfagan las necesidades administrativas de una mejor manera.

NOTA Desde el punto de vista lógico, cada uno de los puertos de un conmutador es un segmento LAN. Los segmentos LAN son los componentes individuales de una LAN separada por un dispositivo de conectividad, como un conmutador.

Por todas estas razones, las redes actuales utilizan los conmutadores para concentrar varios hosts en un único punto de conexión de red (una forma que se llama *configuración en estrella*). Las configuraciones en estrella son los ladrillos con los que se encuentran construidas las redes jerárquicas. En la figura 5-3 se muestran variaciones muy comunes de la topología básica en estrella.

En contraste con los viejos tiempos del trabajo de instalación de cables, la conexión de un host a una red en la actualidad es tan simple como conectar un conector de tipo telefónico. Cada uno de los bloques funcionales de la topología en estrella satisface ciertas necesidades:

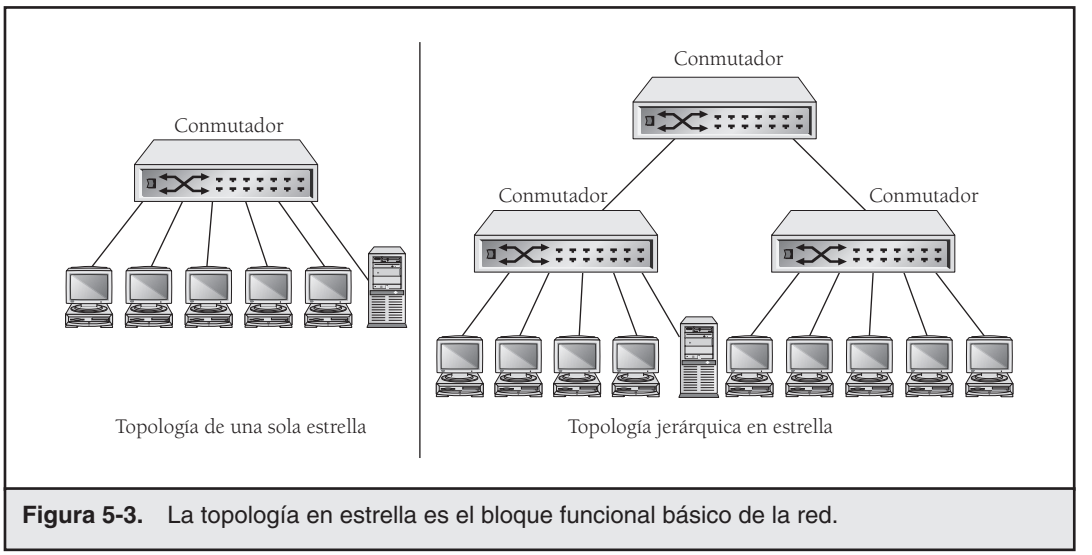


Figura 5-3. La topología en estrella es el bloque funcional básico de la red.

- ▼ Un departamento o pequeño negocio puede utilizar solamente un conmutador para formar una LAN (en efecto, poniendo toda la red dentro de una caja), a lo que se le denomina *topología de una sola estrella*. Con los conmutadores, el cableado de espina dorsal ya no es necesario para formar pequeñas redes.
- ▲ Una *topología jerárquica en estrella* se utiliza para obtener una mayor disponibilidad de puertos de conexión dentro de una oficina. La conexión de conmutadores secundarios (conmutadores de acceso) a uno principal (conmutador principal o de distribución) le brinda a un lugar una mayor cantidad de hosts, para conectarse sin tener que instalar cables adicionales en el área.

NOTA Los términos "espina dorsal" y "troncal central" evocan la imagen de un solo tramo de cable sin rupturas. En realidad, casi todas las espinas dorsales están formadas por muchos tramos de cable unidos entre sí. En el otro extremo, algunas espinas dorsales no están hechas de cable, sino que están contenidas dentro de un gabinete sobre tarjetas de circuito impreso, a las que se denomina espinas dorsales colapsadas. Sin embargo, por definición una espina dorsal es la parte de una red que actúa como la trayectoria principal que enruta el tráfico entre los segmentos LAN. En general, sólo los conmutadores y enrutadores están conectados directamente a las espinas dorsales. En redes grandes, una espina dorsal suele funcionar a una velocidad más elevada que los segmentos LAN que conecta.

La topología de una red está, desde luego, más directamente relacionada con la geografía de la compañía (quién está en qué piso, qué servidor reside en dónde, etcétera, pero hay que tomar en cuenta otras configuraciones). En la tabla 5-1 se muestra una lista de los factores que se deben tomar en cuenta en el diseño de redes y cómo éstos afectan las decisiones acerca de qué hacer cuando se diseñe una red.

Factor	Consideraciones en el diseño de redes
Planta existente de cableado	Para ahorrar tiempo y dinero, a menudo los diseñadores de red tratan de instalar redes sobre cableado que ya fue instalado sobre las paredes y techos de un edificio. A veces no tienen otra opción, y el tipo de dispositivos de red que puede utilizarse lo dicta el cableado existente.
Objetivos de funcionamiento	Las cargas proyectadas de tráfico de la red y la "necesidad de más velocidad" por parte del usuario final pueden influir en la clase de dispositivos de red y la planta de cableado que se vaya a utilizar.
Plataformas	La base instalada de sistemas operativos de red y de plataformas de cómputo, a menudo dictan las decisiones acerca de los diseños de las redes.
Seguridad	Con frecuencia, se utiliza la topología de la red como una forma de ayudar a reforzar la seguridad.

Tabla 5-1. Factores de diseño de la topología (independientemente de la geografía).

Las decisiones de diseño de redes están limitadas muy a menudo por la cantidad de dinero que se desea invertir y por cuestiones logísticas como cuánto tiempo planea la compañía permanecer en un edificio. Por otra parte, las plataformas siempre son estratégicas y generalmente son una condición sobre la que los diseñadores de redes tienen muy poco o nulo control. Si la empresa ha hecho inversiones muy fuertes en NetWare de Novell o SNA de IBM o en Apple, el equipo de la red debe adaptarse a las plataformas de hardware y software que ya se tienen instaladas.

Sin embargo, en la actualidad, sin importar cuál es su presupuesto o qué plataformas esté utilizando, la segmentación de redes es sólo una opción, pero también es el método de diseño preferido.

La importancia de los dominios de red

El *dominio* es uno de los conceptos más importantes de la conectividad. A pesar de que dicho término tiene muchos usos, para nuestros propósitos, lo que es importante son los dos tipos básicos de dominios: el de colisión (o el dominio token en los segmentos LAN Token Ring) y el de transmisión.

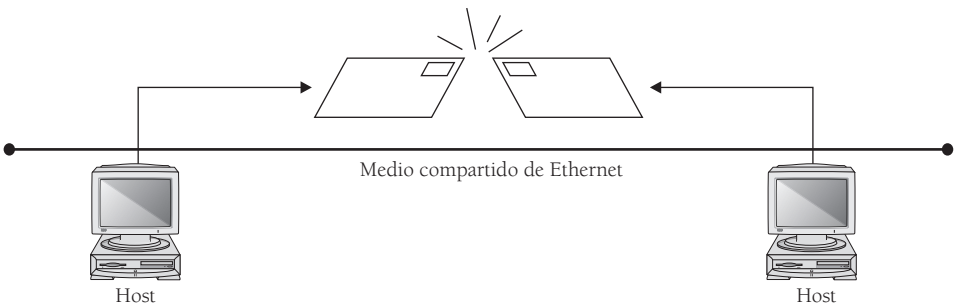
Los segmentos LAN funcionan sobre medios compartidos. En términos físicos, los hosts miembros en un segmento LAN comparten un conmutador. Para eliminar el caos electrónico que de otra forma se presentaría si compartiera un medio y se tratara de "hablar" al mismo tiempo, se debe adoptar una forma de control sobre el acceso al mismo. A esto se le llama *control de acceso al medio* (de donde la dirección MAC toma su nombre, como ya se mencionó).

NOTA Para las personas que toman todo de manera muy literal, pensar que el nombre debería ser "control de acceso al medio de transmisión" (medium access control) porque las LAN, por definición, sólo comparten un segmento conmutado, está en lo correcto (hasta cierto punto). Sin embargo, tenga presente que las direcciones MAC se intercambian entre los diferentes segmentos de manera rutinaria. Además, de alguna forma "control de acceso al medio de transmisión" suena un poco raro en el mundo de las reglas estrictas de la conectividad.

Tanto Ethernet como Token Ring comparten las tecnologías LAN de medio compartido, pero éstas utilizan dos métodos de control de acceso muy contrastante: el método CSMA/CD de Ethernet (acceso múltiple de percepción de portadora/detección de colisiones, Carrier Sense Multiple Access/Collision Detection) y el método de ficha circulante de Token Ring.

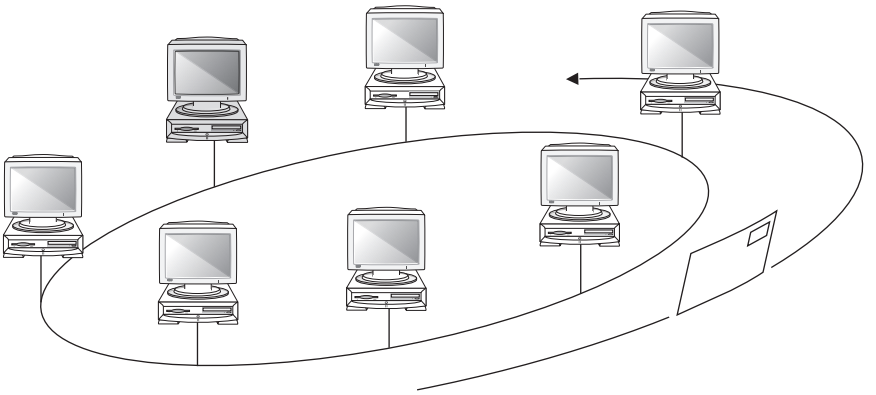
Dominios de colisión en Ethernet

Ethernet permite que los hosts de la red luchen aleatoriamente por el uso del ancho de banda. Un host puede enviar un mensaje a voluntad, pero si éste colisiona con un mensaje enviado por otro host, ambos se dejarán de transmitir y se hará otro intento después de que haya pasado un periodo aleatorio de tiempo. Un dominio de colisión Ethernet es cualquier segmento o puerto en que se presentan colisiones. A medida que haya más tráfico en un dominio de colisión, es mayor la probabilidad de que se presenten colisiones. A la vez, al aumentar el número de colisiones, los hosts tendrán que esperar más y más tiempo para poder retransmitir.



Dominios Token

Un dominio token es el medio compartido de las LAN Token Ring. Token Ring utiliza un método determinístico para controlar el acceso al medio llamado *paso de fichas*. En este método, cada host debe esperar que pase la ficha alrededor del anillo de la LAN antes de que dicho host la tome y transmita. Aunque no se presentan colisiones de paquetes, las LAN Token Ring no son inmunes a la congestión de tráfico. A medida que haya más hosts conectados a un anillo, cada uno de ellos deberá esperar un tiempo mayor para que tenga posesión de la ficha y pueda transmitir. Una buena analogía que ayuda a comprender la tecnología Token Ring es un semáforo en la parte superior de una rampa que lleva a una carretera. Está forzado a esperar la luz verde antes de poder ingresar a la carretera; por tanto, a medida que el tráfico aumenta, deberá esperar más tiempo. No va a atorarse en una congestión en la carretera, pero si el tráfico es muy pesado, deberá esperar algún tiempo en la rampa.



Casi todas las instalaciones LAN nuevas son Ethernet; por ello, en lo que resta de este capítulo, nos enfocaremos en los conmutadores Ethernet y sólo nos referiremos a las Token Ring cuando lo amerite.

NOTA Existen tres tipos de mensajes en las redes que utilizan el protocolo IP: (1) un mensaje de transmisión única es un mensaje enviado a una sola dirección de red; (2) un mensaje de transmisión múltiple es un solo mensaje copiado y enviado a un grupo específico de direcciones de red, y (3) un mensaje transmitido es enviado a todos los nodos de la red. Deberá recordar que las redes IPv6 presentan un cuarto tipo de mensaje, llamado transmisión a cualquier parte. Estos mensajes los transmite un host al host más próximo a él.

Dominios de transmisión

Un dominio de transmisión es un grupo conformado por todas las estaciones (dispositivos de red y hosts) que recibirán cualquier transmisión que se origine en cualquier dispositivo o host dentro del grupo. La diferencia clave entre los dominios de colisión y los de transmisión es que están definidos por el tipo de mensaje que abarcan. Los dominios de colisión abarcan mensajes de cualquier tipo, mientras que los de transmisión sólo abarcan mensajes transmitidos. Como se muestra en la parte inferior izquierda de la figura 5-4, para que los dos conmutadores se conecten al mismo dominio de transmisión, deben estar de alguna manera interconectados (los enrutadores generalmente bloquean los mensajes de transmisión).

En el lado derecho de la figura 5-4 se muestra cómo los dominios de transmisión pueden ser muy diferentes en las redes conmutadas. Utilizando la tecnología de conmutación, un dominio de transmisión puede configurarse específicamente mediante conexiones lógicas en lugar de físicas. A esto se le llama *LAN virtual* o VLAN (Virtual LAN) para abreviar. La palabra "virtual" en VLAN significa que el dominio de la LAN no está definido por su conexión física. En realidad, por lo general las VLAN ni siquiera son locales (más información acerca de ellas se encuentra en la sección "VLAN", en páginas posteriores de este capítulo).

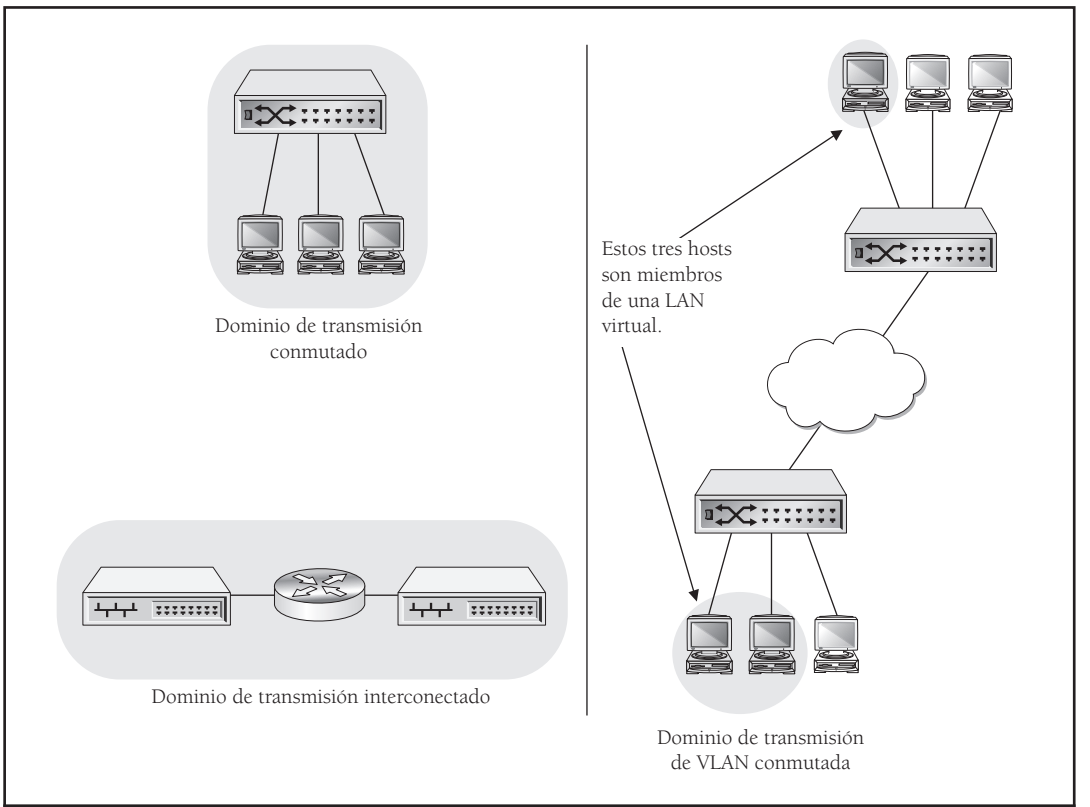


Figura 5-4. Los dominios de transmisión se implementan de manera diferente.

Las colisiones desperdician ancho de banda porque abortan transmisiones. En contraste, los mensajes de transmisión llegan a su destino, pero también desperdician ancho de banda si los hosts de destino los descartan por considerarlos irrelevantes. Evidentemente, los mensajes de transmisión juegan también un papel central en la congestión del tráfico. Piense en los dominios de transmisión como la versión de interconectividad del código postal: a medida que más direcciones se encuentran en un código postal, más tiempo se lleva la entrega de todo el correo. La conectividad no es diferente. A medida que el dominio de transmisión es mayor, la red tenderá a ser más lenta.

La necesidad de segmentar las redes

Los segmentos LAN deben mantenerse de tamaño pequeño como ayuda para garantizar la velocidad de la información útil, limitando la frecuencia de las colisiones. La palabra pequeño también es buena cuando se trata de la flexibilidad, la seguridad y el mantenimiento de la red. La tendencia es dividir las redes en más y más segmentos LAN a medida que el ancho de banda de la red se restringe más y más. Cada vez más usuarios se están convirtiendo en miembros de las redes y, en promedio, los usuarios individuales están generando más tráfico en la red. Además, la mezcla está cambiando a aplicaciones que consumen más ancho

de banda, como imágenes, voz y video. Todas éstas se han combinado para presionar a los administradores de red a entregar más ancho de banda mediante la instalación de medios de transmisión más rápidos y la fragmentación de redes en segmentos aún más pequeños.

Los administradores de red están haciendo ambas cosas, pero la demanda del ancho de banda sobrepasa la habilidad de los fabricantes de redes para crear tecnología más rápida, por lo que las infraestructuras de red están siendo reconfiguradas para incorporar más jerarquización y segmentación. Esta tendencia está reforzada a medida que el costo del hardware necesario para segmentar las redes decae. El refuerzo más grande de esta tendencia es que las herramientas necesarias para integrar y administrar las redes muy segmentadas han mejorado de manera significativa. En realidad, estas herramientas son tan eficientes, que se están utilizando conmutadores para "microsegmentar" las redes en diminutos segmentos LAN.

El cableado define la velocidad y distancia de la red

No puede apreciar la administración del tráfico sin comprender los fundamentos de la construcción de carreteras. Así que, antes de abordar el tema de cómo solucionan los conmutadores de Cisco este problema, es necesario aprender acerca del medio físico en que operan las redes: el cableado.

El aspecto más importante de las redes cableadas es que trabajan con dos tipos de medios físicos de transmisión: el cable de alambre de cobre y el de fibra óptica. Casi todas las redes LAN instaladas en el mundo usan alguna forma de alambre de cobre. El cableado de fibra óptica (a veces llamada *fibra* o *vidrio*, para abreviar) se usa principalmente en espinas dorsales de alta velocidad.

NOTA Aunque el cobre y la fibra son los tipos de medios de conexión que prevalecen, el medio inalámbrico ha cobrado importancia como forma de conectar hosts y dispositivos de red sin tener que estar anclado a un escritorio. En el capítulo 8 se hablará acerca de la conectividad inalámbrica.

La proliferación de los usuarios de redes y las aplicaciones que demandan más ancho de banda, han llevado a la industria a presentar una gran cantidad de tecnologías de transporte nuevas y más rápidas. Un estudio breve del cableado y la terminología de las redes le ayudarán a poner las cosas en orden.

Una breve historia del cableado LAN

Como se mencionó, las primeras LAN trabajaban con cables coaxiales Thicknet. Estos cables eran muy costosos y resultaba difícil trabajar con ellos; por ello, a mediados de la década de 1980, el cable coaxial Thinnet (también llamado *Cheapernet*) se hizo más popular. Cuando se utilizaba en las redes Ethernet a 10 Mbps, Thinnet tenía una longitud máxima de 185 metros. Las LAN Thinnet pueden extender su alcance en distancia utilizando repetidores para conectar segmentos (los *repetidores* son dispositivos colocados a lo largo del cable de la LAN para amplificar las señales eléctricas y extender el alcance de la red. Es muy raro encontrar repetidores en la actualidad). Asimismo, el cable coaxial requiere que exista una cantidad mínima de espacio entre conexiones, lo que disminuye las alternativas para el diseño de la topología.

Los *concentradores* (hubs) se introdujeron a finales de la década de 1980. Hacen posibles las topologías jerárquicas de red y simplifican la instalación y el mantenimiento de la planta de cableado. Los concentradores también aceleraron la introducción de un nuevo tipo de cableado llamado *par trenzado*, que es barato y facilita el trabajo con él. Una de las razones por las que el uso del par trenzado fue posible es que su relativamente corto alcance de 100 metros se puede extender mediante el uso de concentradores. Por ejemplo, a una oficina de 300 metros de longitud podría instalársele par trenzado colocando dos concentradores en la topología.

El cableado de redes LAN en la actualidad

Casi todas las redes grandes en la actualidad utilizan una combinación de fibra óptica y par trenzado. El par trenzado se utiliza para conectar hosts a conmutadores, mientras que la fibra óptica se utiliza para espinas dorsales de red. Gracias a los avances tecnológicos, a pesar de que el par trenzado utiliza menos cobre y protección que el cable coaxial Thinnet, soporta velocidades de transmisión de datos más elevadas. Por las mismas fechas en que el par trenzado estaba reemplazando la tecnología de la conectividad en el escritorio, el cableado de fibra óptica se posicionó como el medio de transmisión de preferencia en las espinas dorsales de red de alta velocidad. La fibra óptica se usa para conectar pisos o grandes áreas en los edificios de oficinas y el par trenzado se utiliza para conectar segmentos LAN que se derivan de la espina dorsal. Como se muestra en la figura 5-5, los conmutadores canalizan los segmentos LAN hacia la espina dorsal mediante las diferentes configuraciones jerárquicas en estrella. Sin embargo, "espina dorsal" es un término relativo. Por ejemplo, a la troncal de fibra óptica que interconecta los edificios de una LAN de campus se le conoce como su *espina dorsal*, mientras que al cable que conecta los pisos de uno de los edificios se llama *elevador*.

El cable de par trenzado es de dos tipos básicos:

- ▼ **STP (Shielded Twisted-Pair, par trenzado con protección)** Un medio de transmisión que consiste en el cableado de dos pares de alambre dentro de una protección aislante para limitar la interferencia electromagnética de señales.
- ▲ **UTP (Unshielded Twisted-Pair, par trenzado sin protección)** Medio de transmisión integrado por cuatro pares de alambre sin protección. El UTP se utiliza en casi todas las redes.

Por lo general, a medida que el torcido del alambre de cobre es más apretado, existe menor probabilidad de que se presente interferencia electromagnética o pérdida de señal en el cable. Como su nombre sugiere, STP tiene una protección que protege el contenido de los alambres. Por otra parte, el UTP no cuenta con protección. Como el UTP es rápido, confiable y barato, se ha convertido en el tipo de cableado predominante utilizado en las redes actuales. El STP es más caro y su uso está limitado a ambientes hostiles en que existen niveles altos de interferencia electromagnética.

Especificaciones del cableado En la tabla 5-2 se explican las categorías del par trenzado que especifica una organización internacional de estándares llamada TIA/EIA (Telecommunications Industry Association/Electronics Industry Association). Estas especificaciones de cableado son importantes porque la velocidad a la que se pueden transmitir los datos de manera confiable está determinada por una combinación de factores, dentro de los que se encuentran:

- ▼ Qué tan apretado está el trenzado de alambre de cobre.
- ■ La calidad del cobre con el que está hecho el cable.
- ■ El tipo de aislamiento utilizado para proteger el cable.
- ▲ El diseño y la calidad de los conectores del cable.

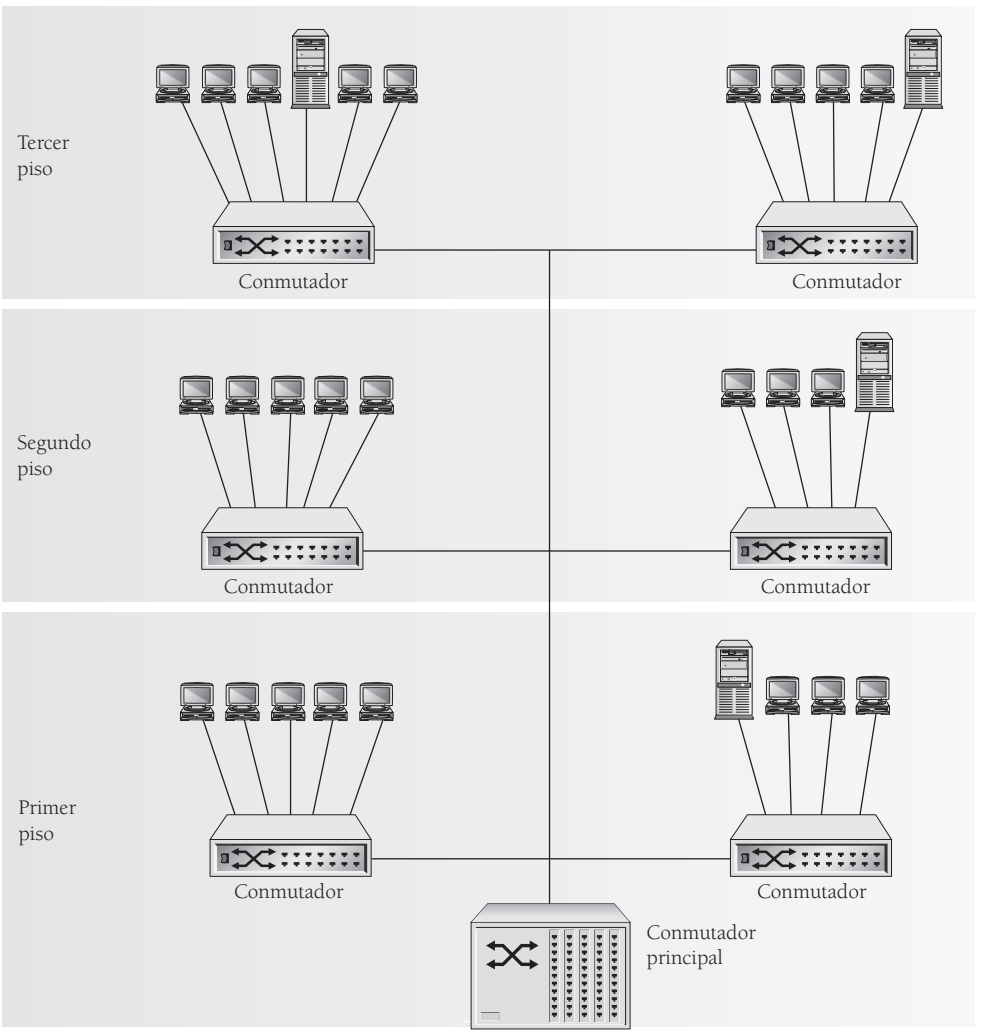


Figura 5-5. Las redes empresariales en la actualidad combinan los medios de transmisión de par trenzado y fibra óptica.

En la tabla 5-2, las categorías 3 y 5 representan la mayor parte de las redes de par trenzado en la actualidad, en especial la categoría 5. Pero échele un vistazo a los cableados relativamente nuevos, Cat 6 y 7. A medida que sea necesario aumentar el ancho de banda, así crecerá su velocidad de adopción.

Observe que los números de categoría más grandes indican velocidades más elevadas. Casi todas las redes LAN actuales utilizan Cat 6 para acomodar Gigabit Ethernet, pero muchas todavía operan con Cat 3, porque éste se encuentra ampliamente instalado en la infraestructura de muchas redes.

La alternativa del cableado con cobre es el cableado con fibra óptica. Aunque se emplea principalmente en espinas dorsales, a veces se utiliza en el escritorio en aplicaciones que

Categoría	Descripción del cable	Aplicación del cable
Cat 1	Cable telefónico convencional.	No se usa para conectividad; ya no se instala en teléfonos.
Cat 2	Cuatro pares trenzados.	4 Mbps; no se recomienda para conectividad.
Cat 3	Cuatro pares trenzados con tres dobleces por pie (30.48 cm) a una velocidad de 16 MHz.	Ethernet a 10 Mbps y Token Ring a 4 Mbps; también se utiliza en cableado telefónico.
Cat 4	Cuatro pares trenzados a una velocidad de 20 MHz.	16 Mbps; utilizado para Token Ring.
Cat 5	Cuatro pares trenzados con ocho dobleces por pie (30.48 cm) a una velocidad de 100 MHz.	100 Mbps; se utiliza para Fast Ethernet; su uso es muy común en edificios que tienen redes instaladas.
Cat 5 Mejorado	Cuatro pares trenzados con ocho dobleces por pie (30.48 cm) pero fabricado con materiales de alta calidad, a una velocidad de 200 MHz.	Diseñado para una capacidad de transmisión de dos veces la del Cat 5 normal.
Cat 6	Cuatro pares trenzados con ocho dobleces por pie (30.48 cm) pero fabricado con materiales de alta calidad. Diseñado para soportar Gigabit Ethernet.	Diseñado para una velocidad de hasta seis veces la de Cat 5 normal.
Cat 7	Cuatro pares trenzados, fabricados con materiales de alta calidad; alcanza velocidades de hasta 600 MHz.	Para aplicaciones de banda ancha a velocidades superrápidas, como Gigabit Ethernet; permite aplicaciones múltiples que operen a diferentes frecuencias.

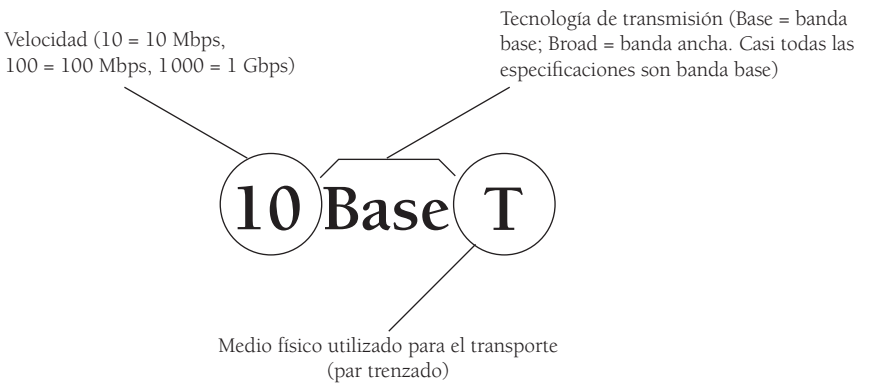
Tabla 5-2. Especificaciones del TIA/EIA para par trenzado.

demandan mucho ancho de banda como las imágenes, aunque Gigabit Ethernet de bajo costo sobre cobre se usa más comúnmente en la actualidad en esos escenarios. La ventaja de la fibra óptica es que puede soportar velocidades de transmisión muy elevadas a distancias considerables, pero su uso está restringido por su relativamente alto costo.

Tecnologías de red Las especificaciones del cableado, como el Cat 6 o 7, describen el medio físico de transmisión. Las *especificaciones de red* describen qué es lo que va a pasar en el medio y están hechas en función a las capacidades y limitaciones de una o más especificaciones del cableado.

Existen varias especificaciones de cableado, cada una de ellas diseñada para garantizar la eficacia del medio físico sobre el que está diseñado para funcionar. La habilidad de cualquier tecnología de conectividad para funcionar apropiadamente depende de lo bien que se adapte al medio de transmisión físico. A medida que la red trabaje a mayor velocidad, o que sea mayor la distancia en que se quiera que opere la red, mejor deberá ser la planta de cableado instalada.

Los nombres de las especificaciones parecen algo misteriosos hasta que comprenda la lógica que hay tras ellas. En la siguiente tabla se analiza el nombre de la especificación 10BaseT de Ethernet.



Poniendo en orden las diferentes especificaciones de red, se ve que algunos medios de transmisión sólo se utilizan a ciertas velocidades, algunas son especificaciones convencionales que ya no se usan en las nuevas instalaciones y otras son especificaciones que nunca tuvieron éxito. En la tabla 5-3 se proporciona una lista de las especificaciones de red (Ethernet, principalmente) en orden aproximado de importancia, con base en:

- ▼ Porcentaje de nuevas LAN que están siendo instaladas.
- ■ Porcentaje de todas las instalaciones.
- ▲ Probable importancia en un futuro como tecnología.

Las especificaciones reflejan la tendencia mundial hacia las tecnologías Ethernet. Las dos excepciones principales son FDDI y ATM.

En la tabla 5-3 se muestra que muchas especificaciones de red son antiguas o que están de acuerdo con estándares que tienen una aceptación limitada en el mercado. La tendencia en la tecnología de la conectividad es, desde luego, hacia velocidades cada vez más rápidas

Especificación LAN	Descripción
10BaseT	Ethernet a 10 Mbps utilizando cableado UTP, Cat 3, 4 o 5; usado en casi todas las instalaciones durante la década de 1990; se encuentra en el proceso de ser desplazado por 100BaseT; 100 metros de límite de distancia.
100BaseTX	Fast Ethernet a 100 Mbps utilizando cableado UTP, Cat 5; casi todas las instalaciones nuevas son 100BaseT; 100 metros de límite de distancia.
100BaseFX	Fast Ethernet a 100 Mbps utilizando dos hebras de fibra óptica multimodo por vínculo; casi todas las espinas dorsales nuevas de alta velocidad son 100BaseFX; límite de distancia: 400 metros.
FDDI	LAN Fiber Distributed Data Interface (interfaz de datos distribuidos por fibra) de paso de fichas a 100 Mbps que utiliza cableado de fibra óptica unimodo o multimodo (o a veces par de cobre STP o UTP, llamado CDDI: Copper Distributed Data Interface, interfaz de datos distribuidos por cobre); límite de distancia de 100 kilómetros por fibra óptica, 100 metros por cobre.
ATM	Asynchronous Transfer Mode (modo de transferencia asíncrona), a 622 Mbps sobre cableado de fibra óptica; es popular como espina dorsal por su eficiencia constante y su habilidad comprobada para transferir aplicaciones multimedia a velocidad.
1000BaseFX	Gigabit Ethernet a 1 Gbps sobre cableado de fibra óptica; aunque 1000BaseX está en proceso de reingeniería para trabajar sobre cobre Cat 5 (se va a llamar 1000BaseTX).
10GBASE-SR	Está diseñado para soportar distancia pequeñas con fibra multimodo en el rango de 26 a 82 metros.
10GBASE-LRM	Está diseñado para soportar distancias de hasta 220 metros sobre cable multimodo.
10GBASE-LR	Está diseñado para soportar fibra unimodo en distancias de hasta 25 kilómetros.
10GBASE-ER	Está diseñado para soportar fibra unimodo en distancias de hasta 40 kilómetros.
10GBASE-LX4	Diseñado para soportar fibras multimodo desde 300 metros hasta 10 kilómetros utilizando fibra óptica unimodo.
10GBASE-CX4	Utiliza conectores InfiniBand de cuatro vías en distancias de hasta 15 metros.
10GBASE-T	Proporciona conexiones a 10 gigabits mediante cables UTP o STP convencionales.
100VG-AnyLAN	Fast Ethernet y Token Ring a 100 Mbps utilizando cableado UTP, Cat 3, 4 o 5; desarrollado por Hewlett- Packard; puede funcionar sobre redes 10BaseT existentes.

Tabla 5-3. Especificaciones LAN de tipos de cable y límites de distancia (*continúa*).

10Base2	Ethernet a 10 Mbps utilizando cableado coaxial Thinnet; se instaló ampliamente en la década de 1980; fue reemplazado por la tecnología 10BaseT; 185 metros de límite de distancia.
10Base5	Ethernet a 10 Mbps utilizando cableado coaxial Ticknet; se instaló ampliamente en las décadas de 1970 y 1980; 500 metros de límite de distancia.
100BaseT4	Fast Ethernet a 100 Mbps utilizando cuatro pares de UTP, Cat 3, 4 o 5; 100 metros de límite de distancia.
10BaseFB	Ethernet a 10 Mbps utilizando cableado de fibra óptica; se utiliza como espina dorsal LAN (no se pueden conectar hosts directamente); 2 kilómetros de límite de distancia.
10BaseFL	Ethernet a 10 Mbps utilizando cableado de fibra óptica; límite de distancia: 2 kilómetros, 1 kilómetro con FOIRL (Fiber-Optic Inter-Repeater Link, vínculo de interrepetidor de fibra óptica, una metodología de señalización precursora que reemplaza a FL).
10BaseFP	Ethernet a 10 Mbps utilizando cableado de fibra óptica; se utiliza para vincular computadoras en una topología estrella sin la utilización de repetidores; 500 metros de límite de distancia.
10Broad36	Ethernet a 10 Mbps utilizando cableado coaxial de banda ancha; 3.6 kilómetros de límite.

Tabla 5-3. Especificaciones LAN de tipos de cable y límites de distancia (*conclusión*).

que funcionan sobre una planta de cableado barata. Sin incluir a las espinas dorsales de alta velocidad, casi todas las LAN actuales utilizan 1000BaseX Fast Ethernet que trabajan sobre cableado Cat 6 o 7.

Las cosas no son tan evidentes cuando se trata de cuál tecnología está ganando como medio de espina dorsal preferido. Tal vez la tecnología ATM sustituyó a la de FDDI, en parte debido al incremento abrupto reciente en la demanda de aplicaciones multimedia. La tecnología 1000BaseX llamada comúnmente Gigabit Ethernet, es el medio de transmisión más popular en la actualidad. A las personas que planean las redes no sólo les gusta la velocidad de Gigabit Ethernet de 1000 Mbps, sino que también les gusta su compatibilidad con casi todas las redes Ethernet instaladas. En el capítulo 2 se estudian de manera detallada las tecnologías de red en competencia.

NOTA ¿Alguna vez se ha preguntado cómo viajan los datos por un cable? En términos simples, los pulsos eléctricos que viajan por un alambre se miden en voltajes positivos o negativos para rastrear las señales. Se utilizan esquemas de codificación especiales (como los del Institute of Electrical and Electronics Engineers [IEEE] para Fast Ethernet y Gigabit Ethernet) para traducir datos a partir de patrones de bits identificables representados por fluctuaciones de voltaje. Fast Ethernet usa un esquema de codificación de tres niveles para rastrear los datos; Gigabit Ethernet utiliza un esquema de codificación de cinco niveles. Los

dos problemas principales que enfrentan las comunicaciones de red son la pérdida por retorno y la interferencia de extremo cercano/lejano. Sin profundizar en los detalles de ingeniería, la pérdida por retorno es cuando una señal hace eco hacia el transmisor, provocando confusión en él; la interferencia, por otra parte, es cuando las señales se escapan entre los pares de alambres, creando ruido eléctrico. Los ingenieros de redes están siempre en busca de mejores esquemas de codificación para incluir más ancho de banda en alambres de menor tamaño. No es como conectar dos botes de lata con un alambre, ¿verdad?

Cables y dispositivos conectados directamente contra conectados cruzados

En la documentación de hardware de red con mucha frecuencia se hace referencia a cables conectados *directamente* y cables *cruzados*. Los dispositivos de red tienen pines de transmisión (TX) y pines de recepción (RX). En un cable conectado directamente, el par de alambre no cruza de TX a RX entre interfaces. Sin embargo, en el cable cruzado, los pares de alambre se instalan cruzados de TX a RX entre conexiones. Se deben utilizar cables cruzados para conectar hosts que tengan interfaces idénticas. Si se utiliza el cable conectado directamente, uno de los dos dispositivos debe efectuar la función de cruzado. Si ningún dispositivo tiene un conector cruzado, entonces se debe utilizar un cable cruzado. En otras palabras, las señales deben estar cruzadas ya sea en uno de los dispositivos o en el cable. En la figura 5-6 se muestran las dos formas.

Imagine que una señal viaja de RX a RX o de TX a TX como una conversación en que dos personas mueven la boca, pero no llega ningún sonido a sus oídos. Las señales cruzadas entre dispositivos hacen posible la conectividad transfiriendo la señal desde "la boca (TX) hasta el oído (RX)".

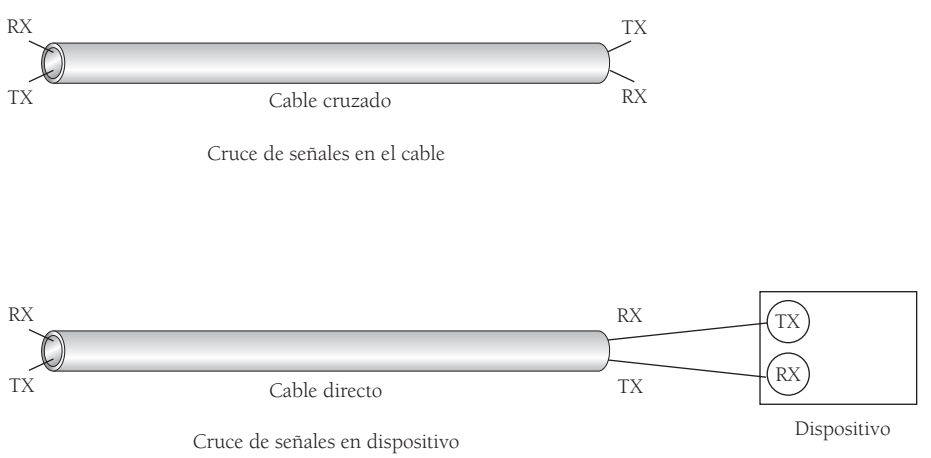


Figura 5-6. Las señales pueden estar cruzadas en el cable o en el dispositivo.

CONMUTADORES CISCO

No es exageración decir que la tecnología de red conmutada está revolucionando la forma como se diseñan las interconexiones y lo que éstas pueden hacer por los usuarios. En la década pasada, los conmutadores comenzaron a ejercer presión sobre las interconexiones, para que éstas adopten métricas y niveles de servicio que muchos consideraban inviables no hace mucho tiempo.

Pero, ¿qué son exactamente las redes conmutadas? ¿Cómo trabajan? Cisco lo pone en estos términos, "Los conmutadores entregan ancho de banda compartido", ¿Cómo hacen esto los conmutadores? La respuesta se encuentra en la electrónica:

- ▼ Se ejecutan a velocidades muy elevadas porque funcionan en la capa de vinculación de datos (capa 2) en lugar de la capa de red (capa 3), donde trabajan los enrutadores. Esto permite que los conmutadores procesen el tráfico sin crear cuellos de botella.
- ▲ Tienen muchas de las capacidades de un enrutador, pero se instalan entre el host y la espina dorsal en lugar de hacerlo entre espinas dorsales, como lo hacen los enrutadores. Los conmutadores pueden tomar el control del tráfico en o cerca de su fuente, mientras que el enrutador generalmente no lo toma sino hasta que el mensaje está listo para comenzar su viaje hacia una LAN remota. El hecho de tomar el control en la fuente, elimina la aleatoriedad de las operaciones en la red.

Cómo funciona un conmutador individual

Casi todos los avances en el campo de las computadoras, de una manera u otra, se resumen en la velocidad y el grado de miniaturización, y el conmutador de la red no es diferente. Los conmutadores son inteligentes y lo suficientemente rápidos para leer el puerto fuente y el de destino en cada marco y "conmutar" mensajes entre los dos (de ahí su nombre). En la figura 5-7 se muestra lo anterior.

De la misma forma que los enrutadores, los conmutadores examinan las direcciones de origen y de destino conforme circulan los mensajes. La diferencia entre los conmutadores y los enrutadores es que, a los primeros les interesan las direcciones MAC de la capa 2 en lugar de las direcciones IP de la capa 3.

El conmutador ofrece una LAN como medio de comunicación compartido a la que pueden conectarse hosts. Sin embargo, el conmutador es, al mismo tiempo, capaz de asumir tareas como poner en orden los paquetes, por dos razones:

- ▼ Los conmutadores poseen una electrónica más potente que sus predecesores, los concentradores.
- ▲ Trabajan en la capa de vínculo de datos (capa 2), lo que significa que no tienen que meterse tan a fondo en los mensajes como los enrutadores de capa 3.

Una electrónica reforzada proporciona al conmutador la capacidad de una lectura más rápida; sin embargo, aunque los conmutadores son inteligentes, no lo son tanto como los enrutadores. En realidad, al conmutador se le asigna una tarea de lectura más ligera que a los enrutadores debido a que maneja tráfico en la capa 2.

Para ilustrar lo anterior, en la figura 5-8 se rastrea un mensaje a través de una red conmutada hipotética. El primer paso se presenta entre el host que envía el mensaje y el puerto

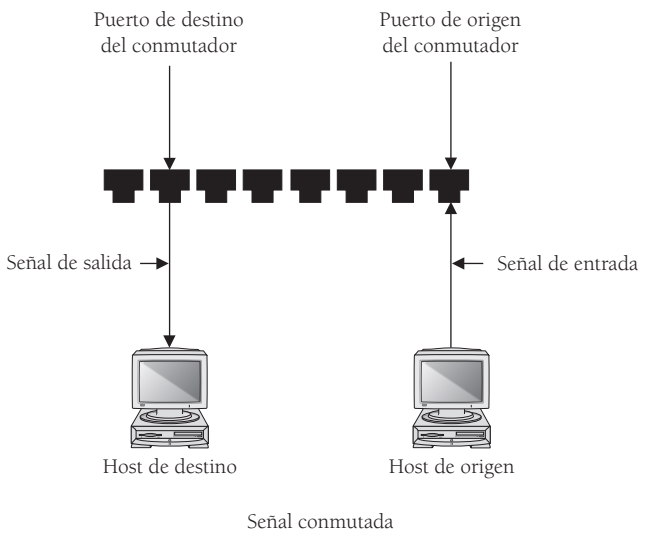


Figura 5-7. Los conmutadores entregan señales a un puerto específico.

de su conmutador. Para esto, el conmutador lee la dirección MAC de destino del mensaje entrante y al instante la transfiere al puerto de salida que está asociado con el MAC de destino.

Debido a que el mensaje se conmuta a un puerto de salida de destino en lugar de ser replicado a todos los puertos, éste no sufre colisiones. Esto hace que haya más ancho de banda disponible y que se muevan los mensajes a velocidades mayores.

El mismo proceso es válido para el segundo paso del mensaje. Conforme el mensaje abandona el puerto de salida del conmutador 1, éste tiene ancho de banda dedicado (no hay colisiones) en el cable que lo conecta al puerto en el conmutador 2. El proceso de conmutación se repite de nuevo a lo largo del tercer paso, hasta el host de destino.

Cuando un conmutador recibe un mensaje que busca una dirección que no conoce, en lugar de eliminar el mensaje, el conmutador lo transmite a todos los puertos. A este proceso se le llama *inundación*, que es necesario para los mensajes de tipo descubrimiento. Por ejemplo, un host utiliza el Dynamic Host Configuration Protocol (DHCP, protocolo de configuración dinámica del host) cuando arranca para localizar servicios que se encuentren cerca, como impresoras de red. Si el proceso de inundación no existiera, los conmutadores no podrían soportar mensajes ampliamente dirigidos enviados por el DHCP y otras utilerías.

Fundamentos de la conectividad conmutada

¿Cómo se puede tener ancho de banda dedicado en una red con varios dispositivos que conecta a cientos de hosts? La respuesta es que las redes conmutadas llevan a cabo un balance entre inteligencia y potencia bruta.

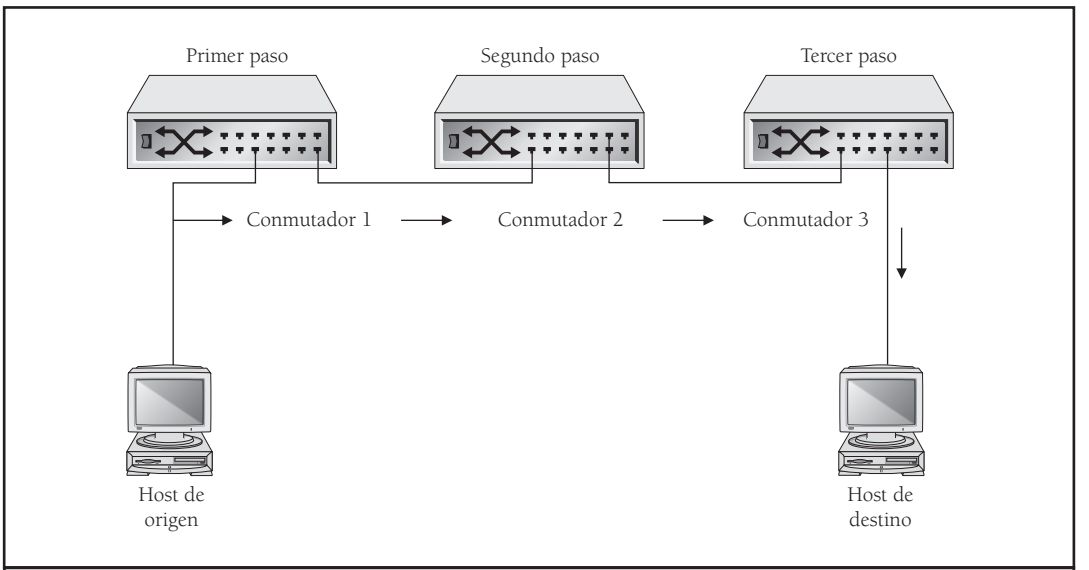
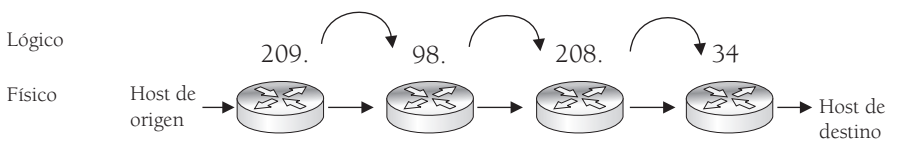


Figura 5-8. Cómo se transfiere un mensaje que circula a través de una red conmutada.

En términos simplificados, los enrutadores transfieren los mensajes a través de una interconexión hacia su destino trabajando de izquierda a derecha con las direcciones IP de destino, como se muestra en la ilustración siguiente:



En sentido general, a medida que el mensaje salta de enrutador en enrutador, éste revisa la tabla de enrutamiento que se conserva en cada enrutador nuevo, tratando de ver si es igual a la de la siguiente parte de la dirección IP de destino. Cuando ve que coinciden, el mensaje se mueve a través de la interconexión hacia el enrutador cuya ubicación está representada por esa información acerca de la dirección IP coincidente. Tarde o temprano llegará el mensaje al enrutador que sirve como la compuerta hacia el host de destino.

En contraste, un mensaje debe encontrar la forma a través de una red conmutada sin el lujo de necesitar direcciones IP jerárquicas. Las redes conmutadas operan utilizando direcciones MAC, a las que se considera de topología plana. Una dirección MAC (también llamada dirección física) es un tipo de número de serie de la red que se asigna a una NIC del host. La primera mitad de cada dirección MAC es un código del fabricante (también conocido como Organizationally Unique Identifier [OUI, identificador organizacionalmente único]) que alude al fabricante de la NIC; la segunda mitad es el número de serie real del dispositivo. Si se lleva un dispositivo al otro lado del mundo, su dirección MAC permanece

inalterada. Las redes conmutadas son completamente planas; como sólo dependen de las direcciones MAC, en esencia piensan que todos los dispositivos y hosts están conectados al mismo cable. Más allá de los confines amigables de la LAN local, una dirección MAC es una pequeña clave. ¿Entonces, cómo manejan los mensajes de entrega las redes conmutadas?

Cuando se enciende un conmutador, éste comienza a construir una tabla dinámica de direcciones. Esto lo hace examinando la dirección MAC de origen de cada marco entrante y asociándola con el puerto del que llegó. Así, el conmutador puede saber cuáles hosts se encuentran conectados a cada uno de sus puertos. En la figura 5-9 se muestra una tabla dinámica de direcciones.

El conmutador también descubre y crea un mapa del entorno utilizando el Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco), que se estudió en el capítulo 4. El conmutador utiliza CDP para descubrir conmutadores vecinos. El CDP sólo se comunica con los conmutadores con los que está directamente conectado, pero como se muestra en la figura 5-10, eso no importa. Las direcciones MAC se envían de regreso por medio de una cadena de conmutadores cooperativos hasta que llegan al conmutador que está haciendo su tabla dinámica de direcciones.

Los conmutadores eliminan los MAC que no se utilizan después de un lapso de cinco minutos. La tabla dinámica de direcciones no es tan inteligente como las tablas de enrutamiento, que utilizan todo tipo de algoritmos para seleccionar las trayectorias óptimas. Un conmutador simplemente coloca los MAC utilizados con más frecuencia en la parte superior de su tabla dinámica de direcciones. En forma conjunta, estos dos procedimientos garantizan que esté activa la inteligencia de los conmutadores de la red para encontrar trayectorias, y que sea confiable.

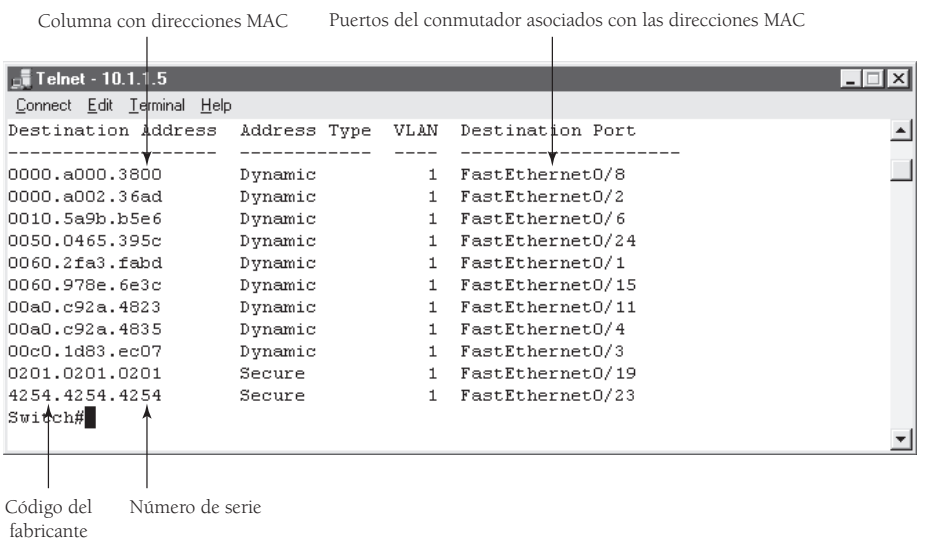


Figura 5-9. El contenido de la tabla dinámica de direcciones de un conmutador es topológicamente plano.

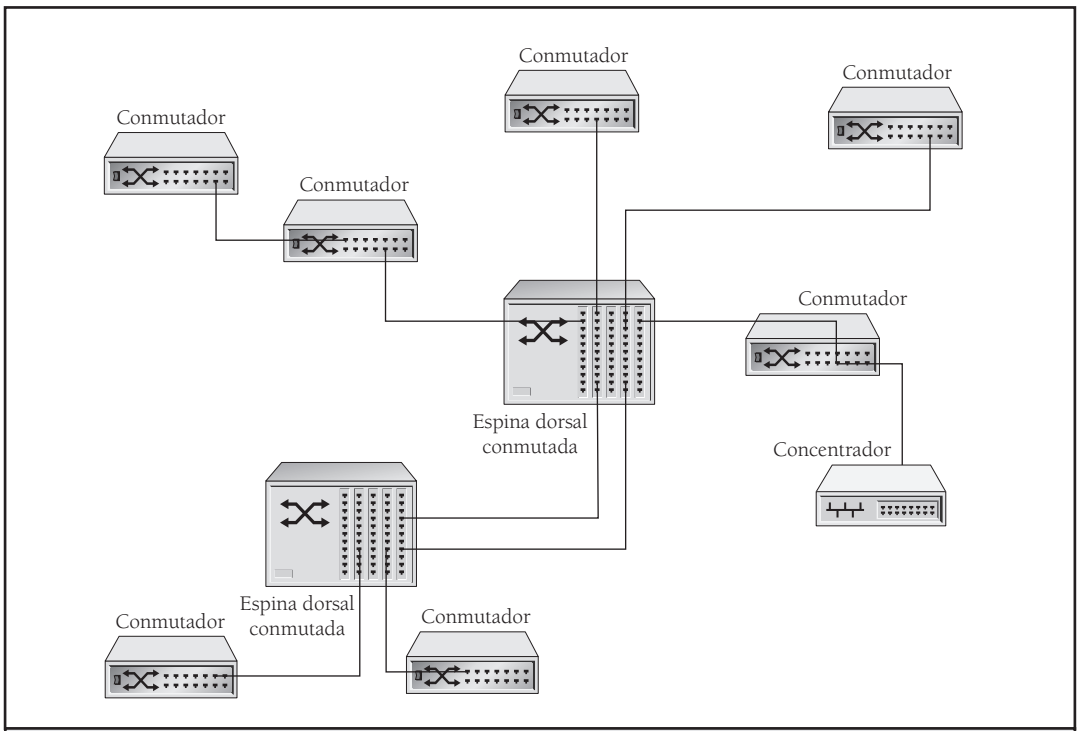


Figura 5-10. Los conmutadores comparten información sobre las direcciones físicas para determinar las trayectorias a través de las redes.

Diseño de interconexiones conmutadas

Aunque la tabla dinámica de direcciones de un conmutador pudiera identificar una trayectoria a través de una interconexión conmutada de gran tamaño, si esa trayectoria requiriera de cientos o aun de docenas de saltos, sería muy lenta. Se han desarrollado dos tecnologías para resolver este problema: las espinas dorsales conmutadas y la conmutación multicapa.

Espinas dorsales conmutadas

Las espinas dorsales conmutadas son conmutadores de extremo superior que se utilizan para agregar ancho de banda desde otros conmutadores. La idea de una espina dorsal conmutada es que ésta tenga la tabla dinámica de direcciones más grande de todas. Las espinas dorsales conmutadas suelen configurarse con varios conmutadores de extremo superior, tanto para propósitos de redundancia como con la finalidad de alcanzar velocidades exageradamente elevadas. El punto principal aquí es ilustrar cómo pueden mejorarse las espinas dorsales.

Sería ingenioso comentarle que las espinas dorsales conmutadas son cables gordos de alta tecnología instalados en la parte superior de las torres de las redes de potencia pertenecientes a las compañías eléctricas, o que son redes de malla con circuitos de datos T3 de muy alta velocidad y costo. Pero no es así. Aun la más grande dentro de las espinas dorsales conmutadas grandes es una colección poco atractiva de cajas tipo refrigerador cableadas entre sí, que se encuentran haciendo un poco de ruido en un cuarto de computadoras lejano.

Una de las tareas de la espina dorsal conmutada es concentrar lo que serían muchos saltos, en un salto a través de una sola LAN de espina dorsal. Las espinas dorsales conmutadas agrupan enormes cantidades de memoria y datos en una sola configuración. No todos los conmutadores de espina dorsal son enormes. Una espina dorsal conmutada podría ser un dispositivo del tamaño aproximado de una caja de pizza ubicada en un estante en un closet de datos. Recuerde que, por definición, una espina dorsal es una LAN relativamente rápida que interconecta otras LAN.

Aunque las espinas dorsales conmutadas no son absolutamente necesarias en redes pequeñas, quizás lo sean en redes muy grandes. Debe recordar cuando la red AOL se colapsó. Después de que sucedió el problema, los gurús vapulearon a AOL por permanecer aferrada por mucho tiempo a su topología que se basaba principalmente en enrutadores.

Las espinas dorsales conmutadas están implementadas utilizando cualquiera de las tres tecnologías:

- ▼ ATM (Asynchronous Transfer Mode, modo de transferencia asincrónica).
- ■ Fast Ethernet o Gigabit Ethernet.
- ▲ 10 Gigabit Ethernet.

Muchas interconexiones de gran tamaño inevitablemente cuentan con subredes que implementan una gran variedad de tecnologías. Por esto, la familia de conmutadores Catalyst 6500 de Cisco posee la característica de conmutación de todos a todos entre ATM, Gigabit, Fast Ethernet y 10 Gigabit Ethernet.

Agregar ancho de banda significa, desde luego, distribuir el tráfico de un determinado número de conmutadores de acceso a otro conmutador más grande y rápido (o a un grupo de conmutadores). Debido a que las redes conmutadas sólo tratan con direcciones MAC, el enrutamiento jerárquico no puede hacer lo anterior. La opción es crear niveles de conmutadores a través de los puertos hacia arriba. En la figura 5-11 se describe cómo esta configuración conduce el tráfico de muchos hosts al conmutador host y luego hasta el conmutador de la espina dorsal.

Esta técnica de configuración permite que los diseñadores generen una jerarquía poderosa a partir de una jerarquía lógica. Las redes conmutadas agregan tráfico al ancho de banda de un solo conmutador para ayudar a que el flujo de tráfico se mantenga. Para describirlo en términos sencillos, esto se lleva a cabo en una máquina de espina dorsal conmutada que tiene más conmutadores conectados directamente a ella y, por tanto, construye una tabla dinámica de direcciones más grande.

La capacidad de cada conmutador Cisco de añadir ancho de banda en una espina dorsal inteligente de alta velocidad depende de todas las tecnologías avanzadas de conmutación que se presentaron en la tabla 5-4.

La tecnología central para la estrategia de espina dorsal conmutado de Cisco es algo que se llama EtherChannel (una tecnología de bus). Hablando estrictamente, un bus es un cable (o una tarjeta de circuito impreso que funciona como cable). Lo que hace de EtherChannel una tecnología de éxito es que representa un paquete integral de cableado de alta velocidad, conectores, controladores, software y herramientas administrativas diseñadas para mantener velocidades de conmutación muy elevadas. EtherChannel proporciona escalabilidad en el ancho de banda en incrementos desde 200 Mbps hasta 80 Gbps.

EtherChannel trabaja permitiendo que grupos de puertos lógicos sirvan como conexiones de alta velocidad entre conmutadores que residan en el mismo lugar. Un grupo Ether-

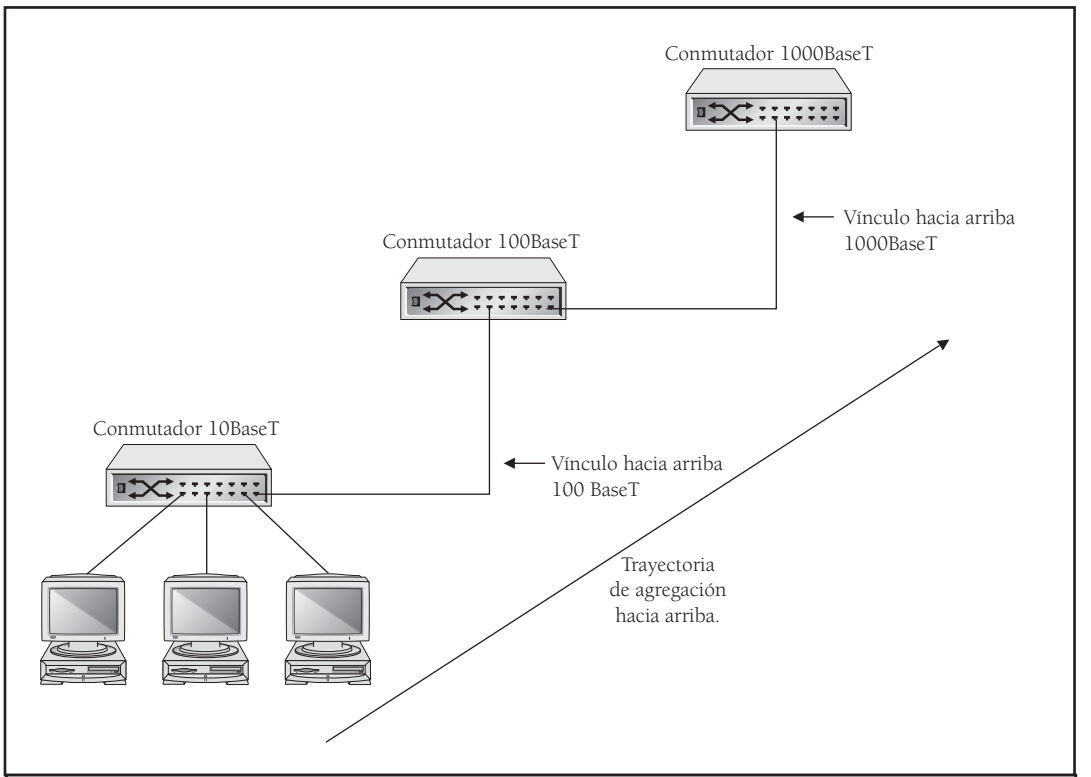


Figura 5-11. Los puertos hacia arriba agregan tráfico a las espinas dorsales conmutadas.

Channel puede tener hasta 12 puertos miembros. Los puertos suelen estar agrupados para dar servicio a una VLAN específica; ésta es la razón por la que EtherChannel es algo primordial en la estrategia de red conmutada de Cisco: agregar ancho de banda significa interconectar conmutadores con servidores de conmutación que almacenen tablas dinámicas de direcciones MAC aún más grandes. Flujos de gran volumen de mensajes conmutados circulan dentro de las VLAN. EtherChannel es donde lo lógico se encuentra con lo físico. EtherChannel conduce el tráfico de una VLAN a través de un bus dedicado de alta velocidad hacia una espina dorsal conmutada colapsada que trabaja a una misma velocidad aproximada. A la velocidad balanceada de transmisión de datos de bus a conmutador se le conoce cada vez más como *tejido del conmutador*, en que los puertos y aun las unidades apilables comparten una tabla dinámica de direcciones común. Por ejemplo, EtherChannel combina el ancho de banda de puertos independientes en un solo puerto. Esto es, un EtherChannel a 600 Mbps en realidad consta de seis interfaces a 100 Mbps.

Un beneficio adicional es que los grupos EtherChannel proporcionan equilibrio y redundancia de cargas. Si un puerto se sobrecarga o falla, las cargas de tráfico se desplazan en forma transparente a otros puertos del grupo. EtherChannel es una arquitectura de diseño que Cisco está utilizando para entregar capacidades de multigigabit. La tecnología implanta

Tecnología	Descripción
Memoria caché de direcciones	También llamada memoria caché MAC (es el número máximo de direcciones MAC que un conmutador puede conservar en su tabla dinámica de direcciones), que está en función de la combinación de factores, incluida la capacidad de la DRAM y la CPU.
Velocidad del cable	También llamada velocidad de reenvío, es la velocidad a la que un conmutador puede aceptar una ráfaga de paquetes de un cable entrante, y se expresa en paquetes por segundo (pps).
Parte trasera (tejido de conmutadores)	La velocidad de datos del bus del conmutador que da servicio a la CPU, la memoria y los controladores E/S, expresada en megabits por segundo (Mbps) o gigabits por segundo (Gbps).
Transmisión múltiple de IP	Ciertos tipos de mensajes tienden a ser transmitidos en varias direcciones; por ejemplo, una copia de un mensaje se envía a 1 000 hosts en lugar de enviarse 1 000 copias. Para hacer esto en una red conmutada se requiere un conmutador con suficiente poder de procesamiento, capacidad de memoria, velocidad del bus y software para manejar transacciones tan grandes de direccionamiento MAC. La transmisión múltiple de IP se está convirtiendo en una tecnología de conmutador a medida que el mundo se mueve hacia el tipo de tráfico que se presta a la mensajería multidirigida, como el video por demanda.

Tabla 5-4. Tecnologías clave de conmutación.

los estándares IEEE 802.3, 100BaseX y 1000BaseX como Fast EtherChannel, Gigabit EtherChannel y 10 Gigabit EtherChannel, respectivamente.

Conmutación de varias capas

La conmutación de varias capas es un híbrido de las tecnologías de enrutamiento y conmutación. Aun las redes conmutadas mejor diseñadas deben utilizar enrutadores en algún nivel. La topología jerárquica del direccionamiento IP de la capa 3 posee un mucho mejor "objetivo" que los esquemas conmutados de red, porque los enrutadores utilizan direcciones jerárquicas en lugar de direcciones MAC planas. Ésta es la razón por la que los diseñadores de redes están usando conmutadores de varias capas para proporcionar a las redes conmutadas las capacidades de un enrutador para identificar y utilizar las trayectorias óptimas hacia sus destinos. Para cerrar con broche de oro, tiene sentido integrar las funciones en una sola plataforma de hardware, siempre que sea posible. Un menor número de saltos y menos "partes móviles" ayuda a mantener las cosas más rápidas y disponibles. Dependiendo del fabricante, a la conmutación de varias capas se conoce también como *conmutación IP, conmutación de la capa 3, enrutamiento de camino corto* y *enrutamiento de alta velocidad*.

Los operadores de interconexiones muy grandes (sobre todo corporaciones que operan intranets grandes) están ofreciendo servicios en que los usuarios pueden hacer clic sobre un hipervínculo en un lugar y, de repente, crear una mensaje que solicite información o servicios de un servidor lejano. A medida que los usuarios conozcan cada vez mejor la interconexión y usen sus servicios remotos, se ejercerá más presión sobre la capacidad de sus enrutadores. Si se implanta adecuadamente, la conmutación de varias capas puede ser diez veces más eficiente en puntos de conexión con elevado tráfico. Lo anterior se debe a que el conmutador puede tomar una decisión de enrutamiento y transmitir datos mucho más rápido que un enrutador.

La conmutación de varias capas trabaja determinando, en primer lugar, la mejor ruta o las mejores rutas para acceder a una interconexión utilizando protocolos de la capa 3 y, después, ordenando lo que encuentre para referencia futura. Los usuarios que lleguen más tarde y deseen circular por esa ruta lo harán a través de los conmutadores, evitando el enrutador (y el cuello de botella que podría provocar).

Aunque la tecnología de conmutación de varias capas no esté integrada en una red conmutada, debería tenerse la capacidad de utilizar parte del enrutamiento para proporcionar alguna forma de topología jerárquica a la red. Esto no sólo es necesario para mantener el nivel de desempeño en toda la red, sino también para mejorar la seguridad. Los conmutadores no desplazarán a los enrutadores de las interconexiones en un futuro cercano. Sin embargo, la conmutación de varias capas podría ser el primer paso de la industria hacia la fusión de lo que en la actualidad son dos tecnologías (de manera muy parecida a como el puente fue absorbido por el enrutador hace cinco o diez años).

VLAN

En una red conmutada, un host puede participar en una VLAN (Virtual Local Area Network, red de área local virtual). De la misma forma en que un grupo de hosts se convierte en miembro de una LAN física al conectarse a un conmutador compartido, también se convierte en parte de una LAN virtual al configurarse en ésta utilizando software para la administración de redes conmutadas. En las redes conmutadas que están construidas utilizando equipo Cisco, las VLAN se crean y mantienen utilizando el software de configuración incluido o el IOS.

NOTA Otra forma de ver una VLAN es pensar en ella como una subred IP. Las dos son sinónimos.

Dentro de una VLAN, los hosts miembros pueden comunicarse como si estuvieran conectados al mismo cable, cuando, en realidad, éstos pueden estar ubicados en cualquier LAN física. Debido a que las VLAN forman dominios de transmisión amplia, los miembros disfrutan de la conectividad, los servicios compartidos y la seguridad asociada con las LAN físicas.

El hecho de basar las LAN en los parámetros lógicos, en lugar de hacerlo en la topología física, brinda a los administradores de red la opción de alinear dominios con grupos de trabajo paralelos, geográficamente dispersos. Aun pueden acomodarse exigencias temporales utilizando VLAN. Por ejemplo, si dos programadores de computadoras necesitaran ejecutar pruebas por toda una semana que involucraran una gran actividad de carga y descarga, podrían configurarse sus equipos como una VLAN para que afectaran el desempeño de los demás miembros de la VLAN normal.

Los dominios se disponen generalmente por departamento o grupo de trabajo. Sin embargo, la tendencia hacia la implementación de estructuras organizacionales dinámicas en el mundo de los negocios, ha hecho que la planeación y el mantenimiento de las redes modernas sea más complejos de lo que serían de otra forma. Los fenómenos que se presentan en los negocios contemporáneos, como oficinas virtuales, equipos distribuidos, reorganizaciones, fusiones, adquisiciones y reducción de la plantilla de personal, provocan una migración casi constante de personal y servicios dentro de las redes. En la figura 5-12 se muestra cómo se vería la topología de una VLAN.

Pero las VLAN son más que una conveniencia organizacional. Son necesarias en las redes conmutadas para extender de manera lógica los dominios de transmisión amplia más allá de la topología física. No olvide que usar solamente direcciones MAC provoca que la topología de la red sea plana. Las VLAN aminoran casi todos los problemas asociados con las topologías planas creando jerarquías virtuales.

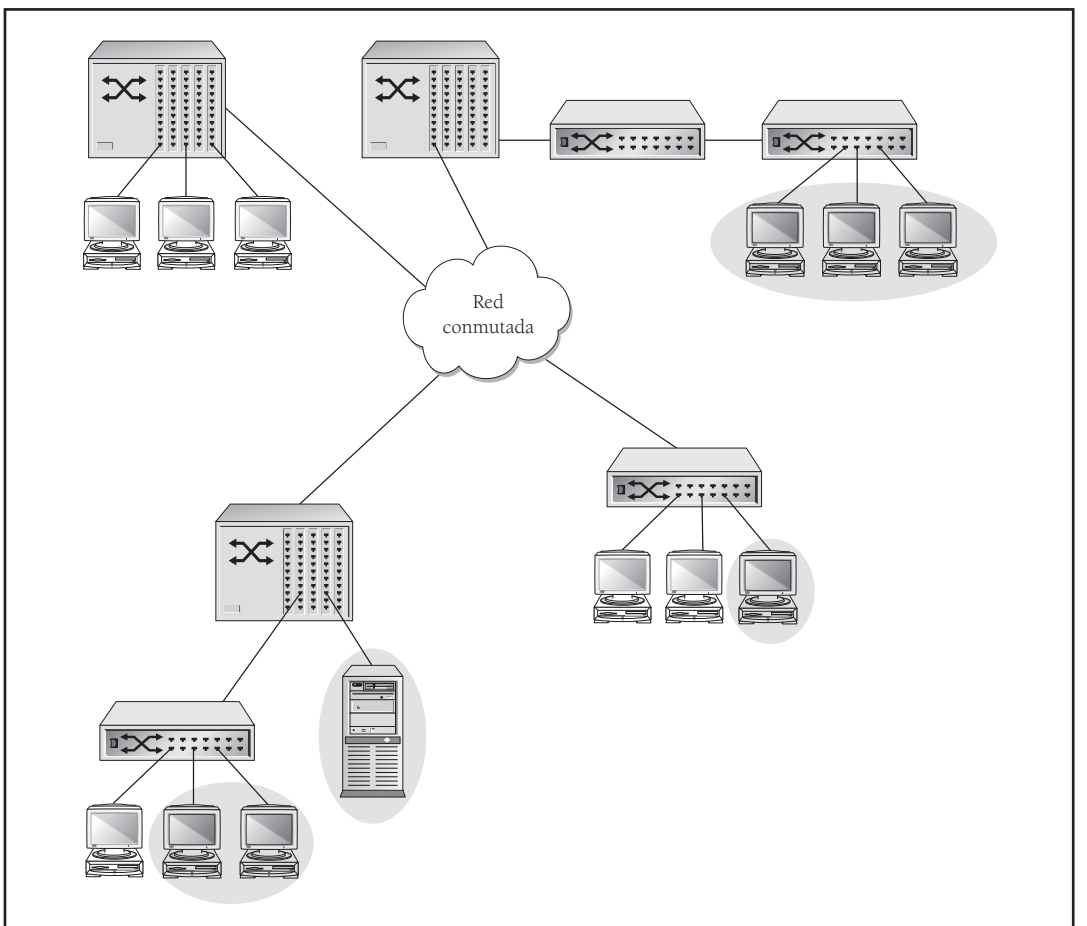


Figura 5-12. Las VLAN ofrecen flexibilidad ilimitada en el diseño funcional de las redes.

Casi todas las VLAN están construidas con conmutadores Cisco. Sin embargo, si un dispositivo de una VLAN necesita comunicarse con otro dispositivo de una segunda VLAN, es necesario utilizar un enrutador (o un conmutador de capa 3). Esto se debe a que dos o más VLAN no pueden comunicarse entre sí (lo que desafía el propósito de la VLAN) sin un poco de ayuda de un dispositivo de capa 3.

Imagine la red que se muestra en la figura 5-13. En este ejemplo, hay dos conmutadores que conectan cuatro VLAN. El conmutador 1 ha sido configurado con las VLAN A y B. El conmutador 2 ha sido configurado con las VLAN C y D.

Las VLAN A y B se envían a través de un solo puerto (se llama *troncal VLAN*) hacia el enrutador y a través de otro puerto hacia el conmutador 2. Las VLAN C y D tienen salida a través de la troncal instalada del conmutador 2 al 1 y después a través de éste hacia el enrutador. Esta troncal puede transportar el tráfico desde las cuatro VLAN. Esa sola conexión hacia el enrutador le permite aparecer en las cuatro VLAN.

Puesto que las VLAN están conectadas al enrutador, pueden comunicarse entre sí mediante la conexión troncal entre los dos conmutadores, utilizando el enrutador. Por ejemplo, si un archivo se encuentra en una computadora de la VLAN D y una computadora de la VLAN A necesita acceso a él, los datos deberán viajar del conmutador 1 al enrutador, y después de regreso a los conmutadores 1 y 2. En términos simples, debido a la troncal, las dos computadoras y el enrutador piensan que están en el mismo segmento físico.

Productos de Cisco para las redes conmutadas

La línea principal de soluciones para redes conmutadas de Cisco son los conmutadores Catalyst, entregados en más de una docena de series de productos diferentes. Debido a la gran cantidad de opciones disponibles, puede "comprarlo a su medida", al menos en lo que se refiere a la conmutación de alta velocidad. La línea Catalyst es similar a los enrutadores Cisco, en el sentido de que incluye modelos de escritorio de configuración fija y modelos de

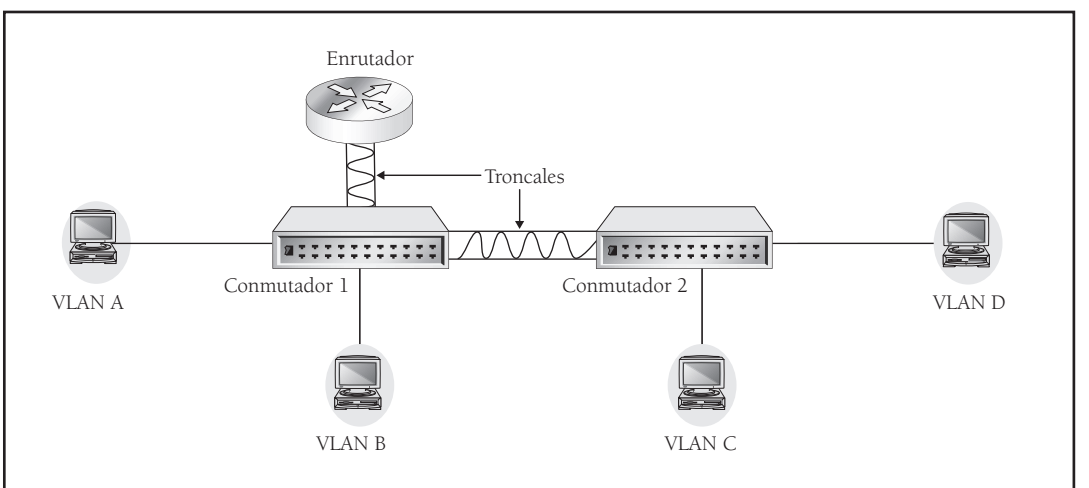


Figura 5-13. Los enrutadores se utilizan para permitir que las VLAN se comuniquen.

chasis modular Plug-and-Play configurables, o paquetes "tamaño refrigerador" con buses de alta velocidad en que pueden insertarse una gran cantidad de tarjetas (cada una de ellas incluyendo otros modelos Catalyst configurados a toda su capacidad).

Para mantenerse actualizado con las tendencias en el mercado de la conectividad, casi todos los conmutadores LAN de Cisco son productos Ethernet. La lista de productos Catalyst para espina dorsal conmutada incorpora la diversidad de tecnologías que compiten a ese nivel, con el soporte para Fast Ethernet, Gigabit Ethernet y ATM.

Casi todos los conmutadores Cisco ejecutan una imagen completa del software del IOS, diferente sólo en que está diseñado para la conmutación y no para el enrutamiento. Casi todos los conmutadores Catalyst ofrecen la interfaz de línea de comandos normal, pero algunos cuentan con una interfaz controlada por menús.

Los productos de Cisco para las redes conmutadas están diseñadas para:

- ▼ Proporcionar una migración sin parches desde las tecnologías convencionales, con herramientas como los puertos de autopercepción 10/100/1000 y puertos de alta velocidad de subida.
- ■ Permitir la interoperabilidad entre diversas tecnologías, como ATM y Ethernet.
- ■ Facilitar la agregación del ancho de banda a través de configuraciones escalables y tecnologías poderosas para la fabricación de conmutadores.
- ▲ Poderse administrar mediante el uso de supervisión remota, configuración y herramientas de seguridad.

En las siguientes secciones se describe la línea de conmutadores de Cisco, actualizada hasta el momento en que se escribió este libro. Consulte la página www.cisco.com para encontrar catálogos de información acerca de conmutadores y otros productos de Cisco.

Conmutadores para LAN Catalyst de Cisco

Un *conmutador LAN* es un dispositivo de capa 2 de alta capacidad que reenvía el tráfico entre segmentos LAN. No se debe confundir con los conmutadores de acceso, como el MicroConmutador o el conmutador Catalyst de extremo inferior, que son dispositivos que conectan hosts a interconexiones de la misma manera que los concentradores. Visto de otra forma, los conmutadores de acceso *forman* segmentos LAN; los conmutadores LAN efectúan la conmutación *entre* ellos.

La familia de conmutadores LAN de la serie Catalyst de Cisco es la más extensa en la industria. Los modelos Catalyst van desde un modelo de cuatro puertos hasta el Catalyst 8500 de clase transportador. La primera clase de la línea de conmutadores LAN Catalyst incluye la serie 2900, que se describe en la tabla 5-5.

La conmutación de varias capas (también llamada conmutación de capa 3) aparece primero en el rango intermedio de la línea de conmutadores Catalyst, como observará en la tabla 5-6. Para reiterar, los conmutadores de varias capas son dispositivos con la capacidad de enrutamiento IP dentro del hardware del conmutador, combinando de esta forma alguna de las capacidades lógicas del enrutamiento IP con la velocidad de conmutación.

Cisco ofrece dos conmutadores de espina dorsal de extremo superior, uno para Gigabit Ethernet y el otro para ATM. Se describen en la tabla 5-7.

Serie del producto	Descripción
Serie Catalyst 2900	Cuatro modelos con 12 a 48 puertos para Ethernet/Fast Ethernet 10/100 de autopercepción. No apilables.
Serie Catalyst 2940	Dos modelos con ocho puertos Ethernet 10/100. El modelo 2940-8TF ofrece Gigabit Ethernet.
Serie Catalyst 2950	Once modelos con 12 a 48 puertos de Ethernet 10/100 y (en la mayoría de los modelo) dos puertos Gigabit Ethernet de subida. Ofrecen funcionalidad inteligente, incluidos los servicios de seguridad y la calidad de servicio (QoS).
Serie Catalyst 2955	Tres modelos, cada uno con 12 puertos. Ofrecen velocidades de hasta Gigabit Ethernet. Este conmutador de calidad industrial se diseñó para usarse en ambientes ruidosos y ofrece las opciones de cobre y fibra óptica. El conmutador es apropiado para aplicaciones militares y para el mercado de empresas prestadoras de servicios.
Serie Catalyst 2960	Cinco modelos con 24 a 48 puertos. Ofrece velocidades de hasta Gigabit Ethernet, tiene una configuración fija y es un dispositivo independiente para empresas nuevas y sucursales.
Serie Catalyst 2970	Dos modelos de conmutadores Gigabit Ethernet de 24 puertos. Estos conmutadores están diseñados para grupos de trabajo y pequeñas sucursales, ofreciendo velocidades de hasta Gigabit Ethernet. El modelo 2970G-24TS también ofrece cuatro pequeños puertos conectables (SFP).

Tabla 5-5. Conmutadores Catalyst de rango intermedio con elevadas densidades de puertos.

Los Catalyst 6500 y 8500 son dispositivos de clase portadora. Tienen una densidad de puertos muy alta para interconectar cientos de segmentos LAN. El 6500 tiene una cuchilla especial que administra la funcionalidad de conmutación de varias capas. La línea 8500 está diseñada para tipos de tráfico multimedia, como VoIP, videoconferencia y otros especializados.

Serie del producto	Descripción
Serie Catalyst Express 500	Cuatro modelos con 8 a 24 puertos. Óptimo para negocios con hasta 250 empleados. Ofrece velocidades de hasta Gigabit Ethernet y proporciona Power over Ethernet (PoE) para simplificar su instalación y uso.
Serie Catalyst 3550	Nueve modelos de conmutadores Ethernet de varias capas apilables. Los modelos ofrecen 24 o 49 puertos Ethernet 10/100 y dos vínculos hacia arriba Gigabit Ethernet.
Serie Catalyst 3560	Ocho modelos con 24 a 48 puertos. Estos conmutadores ofrecen velocidades de hasta Gigabit Ethernet y son dispositivos de clase empresarial de configuración fija.
Serie Catalyst 3750	Cuatro modelos de conmutadores apilables que ofrecen 24 o 48 puertos Ethernet 10/100. Un modelo ofrece 12 puertos Gigabit Ethernet. Los conmutadores utilizan tecnología StackWise, que permite apilarlos con otras nueve unidades 3750.
Serie Catalyst 4500	Cuatro modelos de conmutadores con 3, 6, 7 o 10 ranuras. Cada ranura es capaz de aceptar varios módulos de conmutación ofreciendo 10/100 o Gigabit Ethernet con hasta 240 puertos.
Serie Catalyst 4900	Dos modelos con hasta 48 puertos, esta serie se basa en la serie Catalyst 4500. Estos conmutadores ofrecen velocidades Gigabit Ethernet y también cuentan con dos puertos 10 Gigabit Ethernet.

Tabla 5-6. Conmutadores de rango intermedio con conmutación de varias capas.

Configuración y administración de los conmutadores de Cisco

Los conmutadores Catalyst de Cisco se configuran utilizando la interfaz de línea de comandos del IOS o una interfaz Web, como Visual Switch Manager (VSM) o Cluster Management Suite (CMS). Las preferencias del usuario determinarán el que habrá de utilizarse; ninguno configura nada que el otro no pueda configurar. Si ve la interfaz de línea de comando, se aplican las mismas reglas en cuanto al uso de Telnet para entrar a través del puerto Consola. Por simplicidad, utilizaremos Cluster Management Suite para explicar la configuración y administración de los conmutadores de Cisco.

Serie del producto	Descripción
Serie Catalyst 6500	Cinco modelos con 3 a 13 ranuras. Los conmutadores pueden adaptarse al cliente agregando varios módulos, incluidos Gigabit Ethernet, 10 Gigabit Ethernet, voz, ATM y otros módulos.
Serie Catalyst 8500	Cuatro modelos con 5 a 3 ranuras soportando conmutación ATM multiservicio optimizada para agregar tráfico multiprotocolo. No son apilables. Es la elección de Cisco para conmutadores espina dorsal ATM.

Tabla 5-7. Dos conmutadores Catalyst de extremo superior con troncales gigabit, 10 gigabit y ATM.

CLUSTER MANAGEMENT SUITE (CMS)

Cuando ingresa a un conmutador, tal vez encuentre uno o dos sistemas de administración GUI: Virtual Switch Manager (VSM) o la Cluster Management Suite (CMS). En esencia, estas aplicaciones son las mismas. Aunque superadas por otras herramientas, como el Asistente de Red de Cisco, Cisco Network Assistant (CNA), el CMS aún se utiliza para administrar gran cantidad de conmutadores. Debido a este hecho, hemos optado por incluir aquí una sección acerca de él. Es decir, puede encontrarse algunos conmutadores mucho más antiguos que utilicen VSM. De nuevo, estos programas hacen esencialmente lo mismo y facilitan la configuración y administración del conmutador mediante el uso de una interfaz gráfica de usuario.

Y no se preocupe (si se llegara a preguntar acerca del Cisco Network Assistant) lo estudiaremos con más detalle en el capítulo 13.

Aparte de algunas diferencias básicas acerca de la navegación (en VSM, la configuración se lleva a cabo sobre páginas Web individuales, mientras que en CMS, la configuración se lleva a cabo por medio de ventanas), la diferencia principal entre los dos es que el VSM se basa en HTML, mientras que el CMS se basa en Java. Esto ofrece una GUI más clara, estética y atractiva que su predecesora en HTML. Cualquiera que sea la aplicación con que venga el conmutador que está utilizando, ambas realizan el trabajo.

CMS es una herramienta basada en el navegador Web que trabaja con los conmutadores Catalyst de Cisco. CMS presenta información en tiempo real que mide la actividad en un conmutador mientras está funcionando. Esta información se utiliza para supervisar y administrar un conmutador. Lo que es más importante, la herramienta también se utiliza para modificar la configuración del conmutador.

En la figura 5-14 se muestra la barra de menús del CMS y una lista de páginas por área. La página de inicio en sí misma maneja tareas domésticas como asignar nombre al conmutador y configurar su contraseña de línea.

Una característica sobresaliente de CMS es que el estado del dispositivo puede verse observando una imagen en vivo de dicho dispositivo en la página de inicio. En la figura 5-15 se muestra la imagen gráfica de un conmutador 2950-24 de Cisco. No verá las claves a color en este libro en blanco y negro, pero si el puerto está en verde, su estado es vínculo funcionando; azul significa sin vínculo y rojo indica vínculo con falla o puerto deshabilitado.

Observe que en la figura 5-15 el CMS hace la distinción entre un puerto y un vínculo. Un *puerto* es la conexión física donde el cable se conecta. Un *vínculo*, por otra parte, es la conexión lógica que está realizándose de ese puerto hacia otro, en algún otro dispositivo (que podría ser otro conmutador, enrutador, servidor u otro dispositivo). Un puerto podría estar trabajando adecuadamente y, al mismo tiempo, el vínculo que pasa por dicho puerto podría estar funcionando mal. Observe cómo Visual Switch Manager ayuda a los administradores de red a aislar y resolver problemas rápidamente.

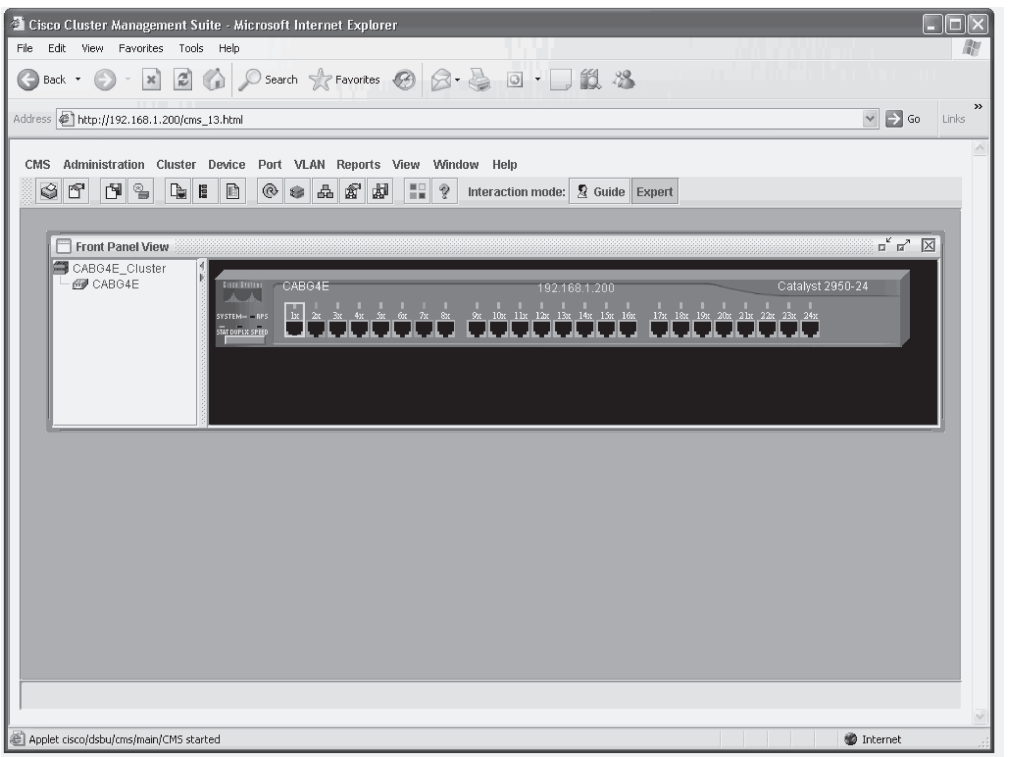


Figura 5-14. La barra de menús del CMS se utiliza para navegar por las opciones de configuración del conmutador.

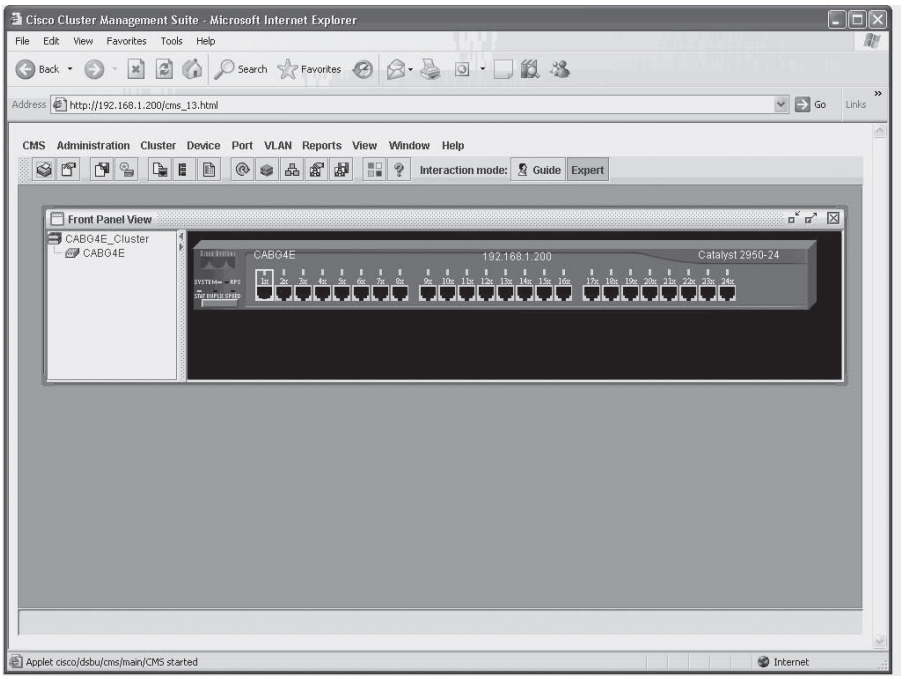


Figura 5-15. Una imagen gráfica en "vivo" reporta un estado del conmutador de Cisco.

Las páginas de configuración del puerto, Port Configuration (o comandos, si se encuentra en la interfaz de línea de comandos del IOS) le permiten habilitar o deshabilitar puertos específicos del conmutador y fijar el modo dúplex a *full*, *half*, o selección automática, de acuerdo con la capacidad del dispositivo host que realiza el vínculo hacia el puerto. Si el dispositivo conmutador que se está configurando es 10/100, el modo velocidad puede fijarse de la misma forma. Si un conmutador está participando en un EtherChannel, se podrían asignar puertos individuales a los grupos EtherChannel en la página Port Grouping.

Las páginas de las áreas administrativas abarcan los parámetros básicos de configuración de todo el sistema, como la versión del software del IOS que está instalada, el procedimiento de arranque, la velocidad de la consola del sistema en bauds y las opciones de configuración de memoria.

Quizás el área más importante de la administración y configuración del conmutador tiene que ver con las VLAN. El Visual Switch Manager incluye páginas para asignar a los puertos membresías VLAN, así como páginas para establecer parámetros de servicios VLAN especializados como:

- **STP (Spanning Tree Protocol, protocolo de árbol expandido)** Es un protocolo de administración de vínculo que permite la publicación de trayectorias redundantes a través de las redes conmutadas, al mismo tiempo que evita que las

trayectorias regresen a su origen. El STP hace para las redes conmutadas lo que los protocolos de enrutamiento hacen para las redes enrutadas.

- **VTP (VLAN Trunk Protocol, protocolo de troncales VLAN)** Es una forma de crear trayectorias que den servicio a varios conmutadores en una VLAN, que se logra compartiendo dinámicamente las direcciones MAC y otra información desde un servidor VTP y clientes VTP.
- **VMPS (VLAN Membership Policy Server, servidor de directiva de membresía VLAN)** Es un protocolo basado en la arquitectura cliente-servidor que rastrea dinámicamente la VLAN (o las VLAN) a la que pertenece una dirección MAC particular.
- **VQP (VLAN Query Protocol, protocolo de consulta de las VLAN)** Es un protocolo que continuamente trabaja estadísticas acerca de las consultas VMPS enviadas por el servidor VMPS a sus clientes.

En el capítulo 13 se conocerán más detalles acerca de cómo pueden configurarse y administrarse los conmutadores utilizando SNMP y CiscoWorks.

Software del Cluster Management Suite

El CMS trabaja comunicándose con un conmutador a través del protocolo HTTP. El HTTP es el protocolo IP que se utiliza para soportar aplicaciones basadas en el navegador Web. Como una aplicación de navegación, el CMS abarca la imagen del conmutador del software IOS de Cisco y trabaja los comandos IOS.

La instalación inicial del conmutador se lleva a cabo mientras funciona una sesión de terminal a través del puerto Consola del conmutador (no el CMS). Observe que tanto Telnet como el Cluster Management Suite son opciones en la figura 5-16. Es solamente hasta después de que el conmutador se hace miembro de una LAN que la actividad de administración puede comenzar con la ayuda del VSM.

La página inicial también proporciona acceso a otras herramientas, aparte del CMS. Por ejemplo, hacer clic sobre el hipervínculo Telnet le permite acceder a la interfaz de línea de comandos del IOS. Otros hipervínculos se conectan a recursos de Cisco, como la página Web de Cisco y el centro de asistencia técnica.

Página inicial de la Cluster Management Suite

La página inicial del CMS es donde el administrador del sistema comienza y es el punto de arranque para todas las actividades de administración del conmutador. Por ejemplo, bajo el menú Administration, puede mirar y cambiar la dirección IP del conmutador y actualizar el firmware del dispositivo.

Los conmutadores están casi siempre administrados desde dentro de la red privada empresarial. En la figura 5-15 se muestra una dirección IP privada (http://192.168.1.200), en contraste con una dirección pública (como http://209.98.86.52). Por razones de seguridad, es raro el acceso administrativo a un conmutador desde fuera de la red privada.

Cuando selecciona un artículo para administrarlo desde la barra de menús, aparece una nueva ventana y generalmente despliega información actual de la configuración. También puede cambiar un parámetro si así lo desea. Para que un cambio en un parámetro surta efecto en el archivo de configuración del conmutador, se debe hacer clic sobre el botón Apply.

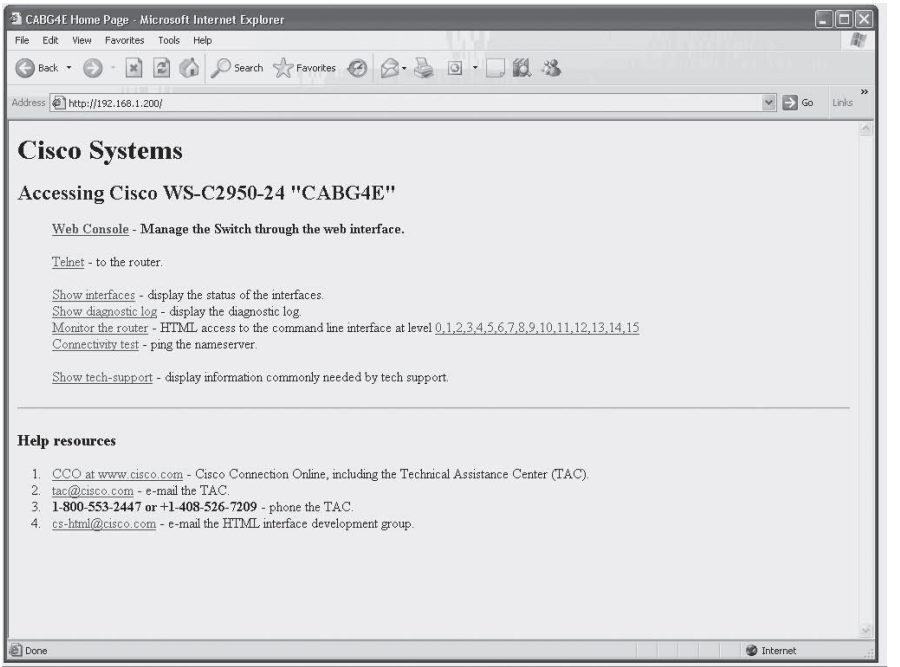


Figura 5-16. Usted accede a la Cluster Management Suite por medio de esta página.

Esto provoca que el cambio en el parámetro sea cargado en el conmutador y actualizado en la memoria del dispositivo.

El dispositivo gráfico interactivo en la Cluster Management Suite

La Cluster Management Suite comienza con una imagen de un conmutador en la parte inferior de la página de inicio. La imagen es del dispositivo conmutador real. El ejemplo de la figura 5-15 está cargado en un Catalyst 2950-24 de Cisco. La imagen del conmutador está "viva", en el sentido de que la información del estado desplegado refleja lo que está sucediendo en realidad en el dispositivo. Cada puerto del conmutador está encendido con uno de los tres colores que indican el estado actual del dispositivo:

- ▼ **Verde** El vínculo está funcionando.
- ■ **Azul** Se reporta ausencia del vínculo.
- ▲ **Rojo** El vínculo está fallando o deshabilitado.

Sin embargo, la imagen del conmutador hace más que sólo reportar el estado del dispositivo. Es una interfaz interactiva mediante la cual puede modificar los parámetros de la

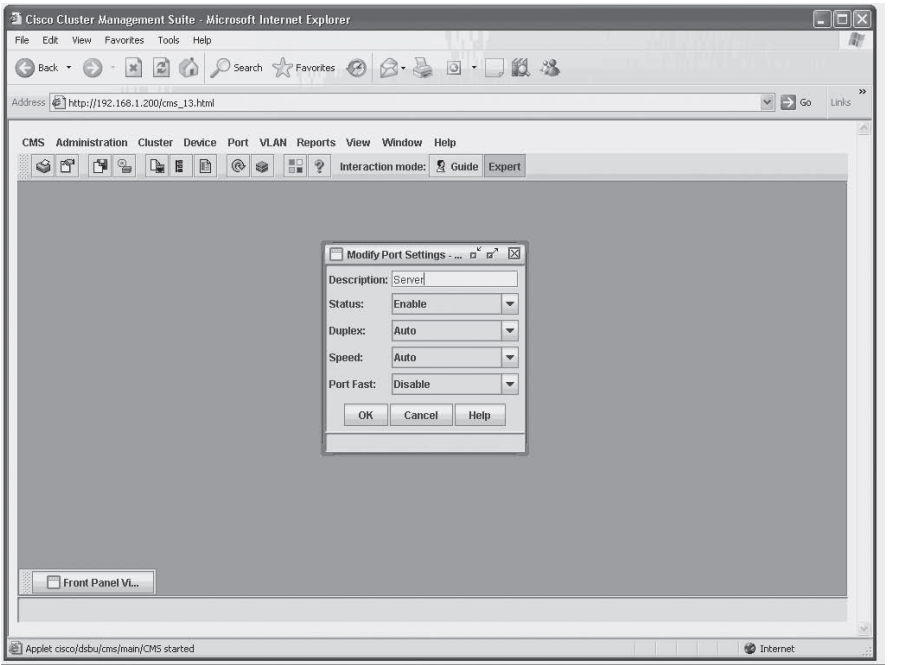


Figura 5-17. Haga clic sobre la imagen del conmutador CMS para configurar puertos específicos del conmutador.

configuración. Si ya leyó la edición anterior de este libro, reconocerá la imagen del conmutador como la misma interfaz de dispositivo gráfico interactivo que se utilizó con CiscoView. CiscoView (que se estudia en el capítulo 15) es un súper conjunto del CMS, en el sentido de que maneja todos los dispositivos Cisco, no sólo los conmutadores.

El cuadro de diálogo de la figura 5-17 aparece después de que el usuario hace clic con el botón derecho sobre el puerto FastEthernet 0/7 en la imagen del conmutador de la figura 5-15 y, después, selecciona los parámetros del puerto del menú contextual. Este cuadro de diálogo de entrada es específico del puerto sobre el que se hizo clic.

Los parámetros básicos del puerto se establecen aquí. El menú desplegable Status enciende o apaga el puerto del conmutador seleccionando Enable o Disable. También puede detectar si el puerto debe ser full-duplex o half-duplex, a qué velocidad debe funcionar (10 Mbps, 100 Mbps o automatic), y si el puerto rápido debe ser habilitado o deshabilitado.

Topology View (Vista de la topología)

La característica Topology View es una aplicación que descubre y diagrama la topología de red en el entorno. Network View *sólo* hace diagramas de dispositivos de Cisco. Proporciona reportes acerca de los dispositivos y vínculos de red y puede utilizarse como una interfaz

interactiva para modificar los parámetros de configuración del dispositivo. Los diagramas del Topology View incluyen las características siguientes:

- ▼ **Visual Stack (Pila visual)** Utilice esta característica para desplegar una imagen del conmutador de uno o más miembros de una pila de conmutadores.
- ■ **Switch Manager (Administrador del conmutador)** Haga clic con el botón derecho sobre un conmutador en la imagen para mostrar un menú contextual con dos opciones: ver un reporte acerca del conmutador o lanzar una aplicación de software de administración que puede utilizarse para reconfigurar la LAN.
- ■ **Link Report (Informe del vínculo)** Haga clic con el botón derecho sobre un vínculo (la línea que conecta los dispositivos en el diagrama) para ver las direcciones IP del vínculo, el modo de operación, las VLAN y otros parámetros de operación.
- ▲ **Toggle Labels (Etiquetas de botón)** Utilícelas para modificar las etiquetas de dispositivo en el diagrama desde direcciones IP hasta los números de modelo de dispositivos de Cisco (por ejemplo, desde la dirección IP 192.168.1.200 hasta el número de modelo 2950-24) y para etiquetar vínculos de red (líneas). Las etiquetas de línea contienen el nombre de la interfaz de dispositivo a través del cual el vínculo está trabajando (por ejemplo, Ethernet1).

Tenga cuidado antes de arrancar Network View. Es probable que sea lento debido a que utiliza el CDP (Cisco Discovery Protocol, protocolo de descubrimiento de Cisco), para

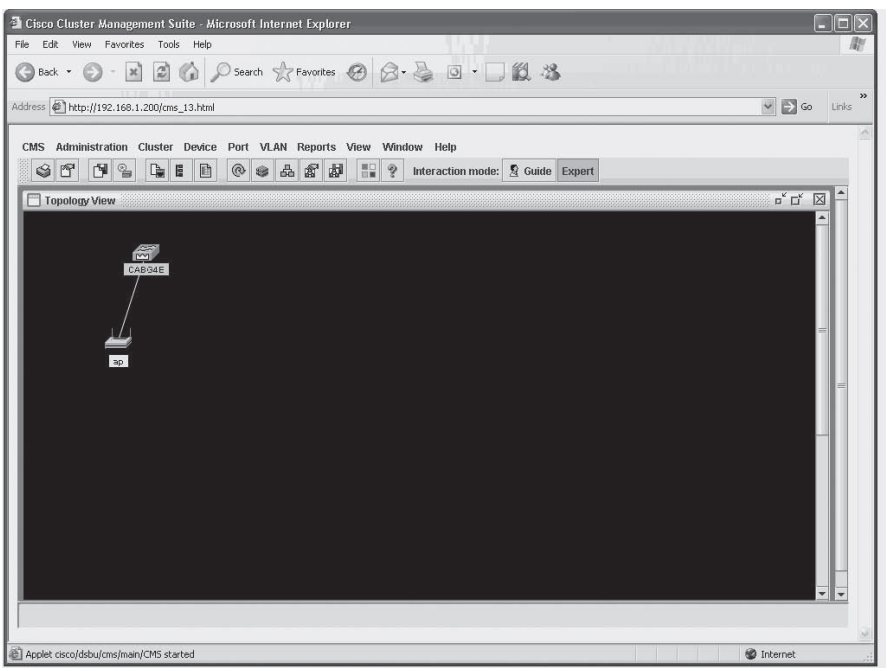


Figura 5-18. El CMS puede construir un diagrama gráfico del conmutador de la LAN.

encontrar otros dispositivos. En la figura 5-18 se muestra la vista de topología de una LAN muy pequeña.

Configuración del puerto del conmutador

Un puerto es donde las estaciones se conectan físicamente al conmutador. Los puertos en los dispositivos conmutadores se llaman *puertos del conmutador* o *puertos conmutados*. Son las conexiones en que se conectan los cables de par trenzado provenientes de los hosts (como PC, servidores e impresoras). Otros dispositivos de red, como los enrutadores y otros conmutadores también se conectan a los puertos del conmutador.

Los puertos del conmutador tienen estatus administrativo y real. Puede accederse a ellos seleccionando Port Settings del menú Port, como se muestra en la figura 5-19. El estatus se fija en el modo Enable, como opción predeterminada. El valor Enable significa que el puerto está listo para trabajar. Actual status (que se muestra en la ficha Runtime Status en la figura 5-20) puede estar tanto en Up como Down. Es posible que el estado administrativo de un puerto esté en Enabled y el real en Down. Esto indicaría que el puerto está listo operativamente, pero sin funcionar (Down) porque no hay ningún dispositivo conectado a él.

Se pueden configurar dos parámetros para afectar la velocidad de operación efectiva del puerto de un conmutador: modo dúplex y transmission speed.

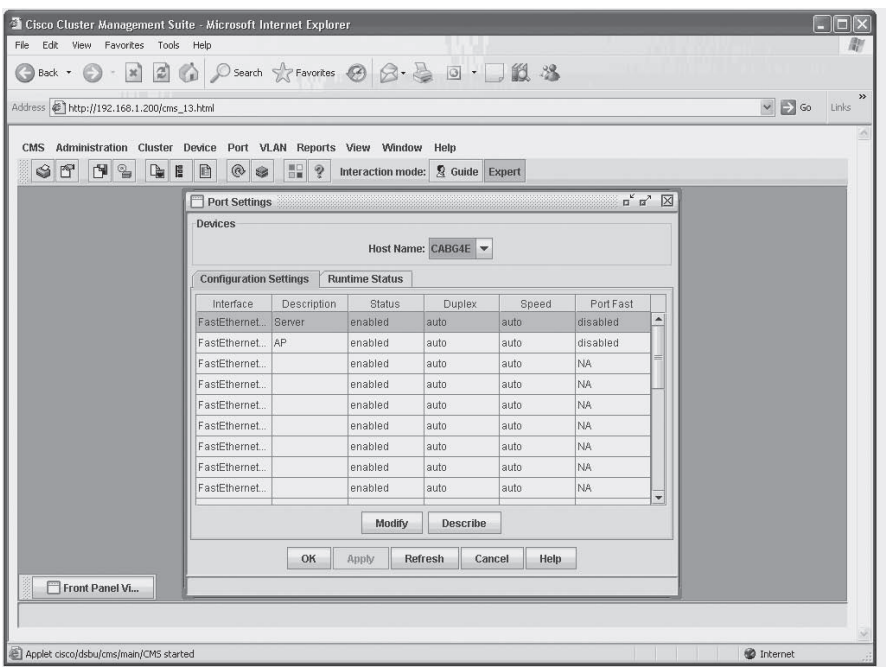


Figura 5-19. Aquí se configuran los puertos individuales del conmutador.

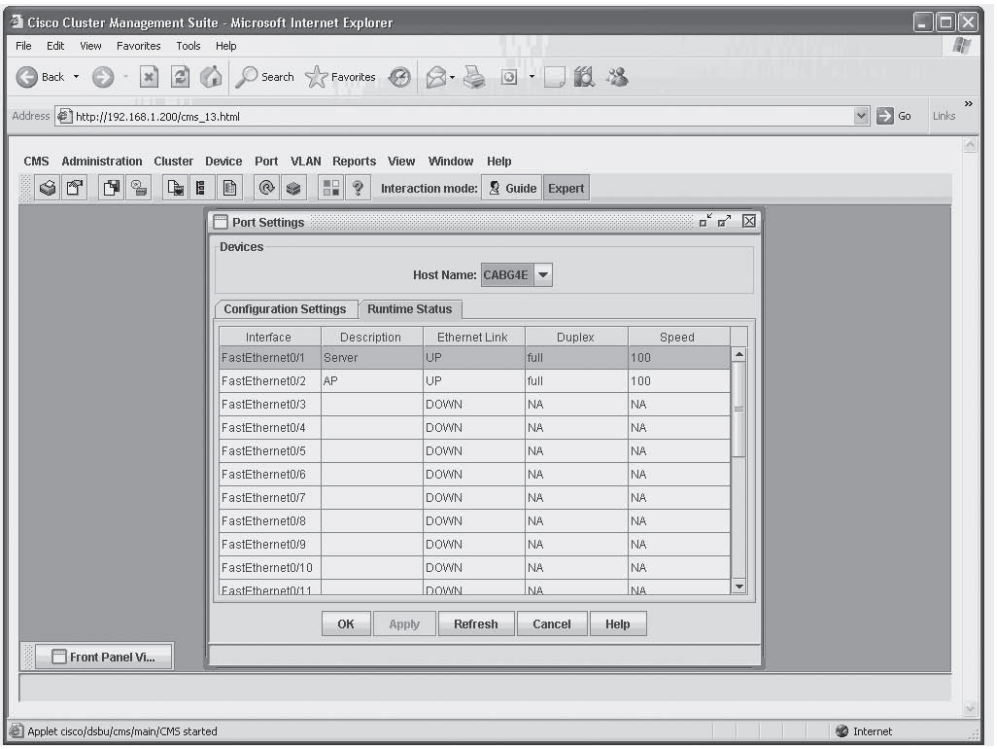


Figura 5-20. Aquí se monitorea el estatus de los puertos individuales del conmutador.

El parámetro Dúplex puede configurarse de tal manera que reconozca automáticamente y fije cualquiera de los modos full-dúplex y half-dúplex. El modo duplex es si la transmisión es en una dirección o en dos. Si los dispositivos conectados a ambos extremos de un vínculo tienen la capacidad de full-dúplex, el parámetro Auto automáticamente pondrá el valor full-duplex, duplicando efectivamente la velocidad de transmisión. A menos que se configure de otra manera, el VSM autonegocia el modo full-duplex siempre que sea posible.

En los conmutadores que cuentan con el autopercepción 10/100, el parámetro Transmission Speed Requested (Velocidad de transmisión solicitada) generalmente se fija en Auto. El término 10/100 se refiere a la capacidad de un conmutador de detectar automáticamente si el dispositivo en el otro extremo del vínculo está funcionando a 100 Mbps (Fast Ethernet) o a 10 Mbps (puro Ethernet). Al menos que esté configurado de otra forma, el CMS autonegocia una conexión a 100 Mbps siempre que sea posible. Los administradores de red harán caso omiso de Auto y especificarán una velocidad sobre la otra cuando el conmutador tenga problemas para detectar correctamente la velocidad de un vínculo.

Agrupamiento de puertos

Los *grupos de puertos* son conexiones lógicas de alta velocidad entre conmutadores. Están configurados para conexiones Fast EtherChannel o Gigabit EtherChannel. Los grupos de puertos crean vínculos redundantes entre conmutadores, de tal forma que si existe una falla con un vínculo del grupo, su tráfico se moverá automáticamente a los demás vínculos (un proceso automático llamado *recuperación de fallas*).

Un grupo de puertos se trata como un solo puerto lógico. La formación de grupos de puertos simplifica la administración y los informes. Por ejemplo, los cambios de configuración de un puerto necesitan hacerse en un solo punto en lugar de cada puerto individual. En la figura 5-21 se muestra la interfaz para formar grupos de puertos. Ésta se puede encontrar seleccionando EtherChannel del menú Ports.

Todos los puertos en el grupo deben pertenecer al mismo conjunto de VLAN, y todos deben basarse en el origen o el destino, lo que se muestra en el menú desplegable ubicado en el centro de la ventana de la figura 5-21. La conmutación *basada en el origen* es cuando el grupo de puertos toma decisiones de conmutación con base en los MAC de destino. En la conmutación *basada en el destino*, las decisiones de los conmutadores están basadas en los MAC de destino. Es correcto configurar los grupos de puertos basados en el origen y los basados en el destino en el mismo conmutador, pero no en el mismo grupo.

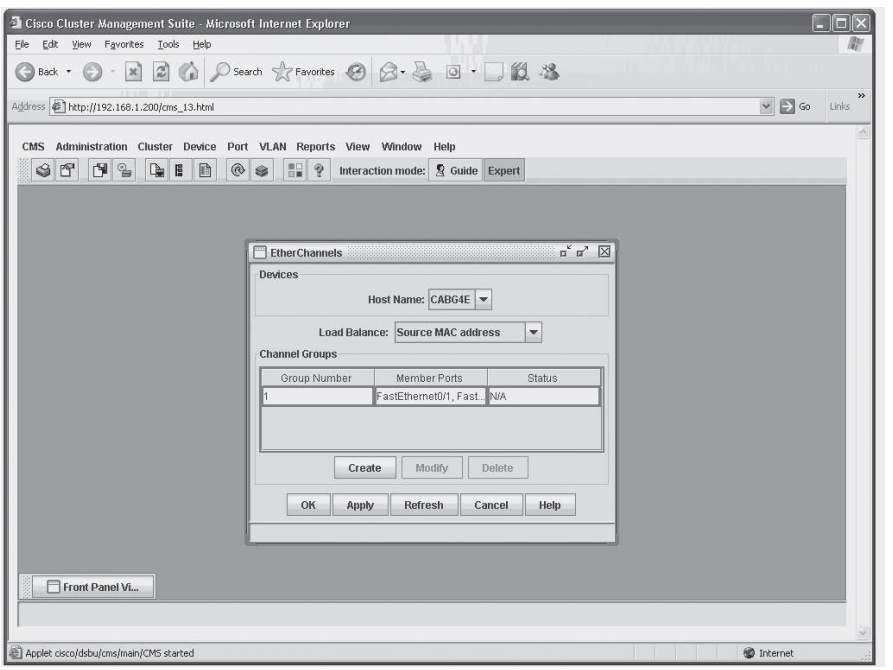


Figura 5-21. Los grupos de puertos EtherChannel se configuran en cuanto a velocidad y redundancia.

Monitoreo de puertos (SPAN)

El SPAN (Switched Port ANalyzer, analizador de puertos conmutados) reúne información en tiempo real para el monitoreo de los puertos del conmutador y el diagnóstico de problemas. Su propósito es concentrar información acerca de la actividad del puerto en un solo puerto (el puerto SPAN) dedicado a la reparación de fallas. Un puerto SPAN funciona como un instrumento de prueba, pero en la forma de un puerto dedicado del conmutador en lugar de hardware independiente desde un dispositivo externo de prueba.

SPAN trabaja haciendo un espejo del tráfico desde uno o más puertos del conmutador hasta el puerto SPAN. Si los puertos que se están monitoreando son miembros de una VLAN, el puerto SPAN debe ser un miembro de la misma VLAN. En la figura 5-22 se muestra que se están monitoreando dos puertos en el conmutador de ejemplo. Se accede a la ventana de diálogo SPAN seleccionando SPAN en el menú Ports.

El puerto SPAN opera el software de prueba RMON. *RMON* (Remote Monitoring, monitoreo remoto) es un software de prueba especializado que rastrea las estadísticas de desempeño del puerto, los patrones de tráfico y las alarmas. Por lo general, una tarjeta llamada Network Management Module (NMM, módulo de administración de red) se inserta en el conmutador para proporcionar la electrónica que se encarga del monitoreo y el diagnóstico de problemas. A veces, una estación de administración de red lee datos desde el puerto y no

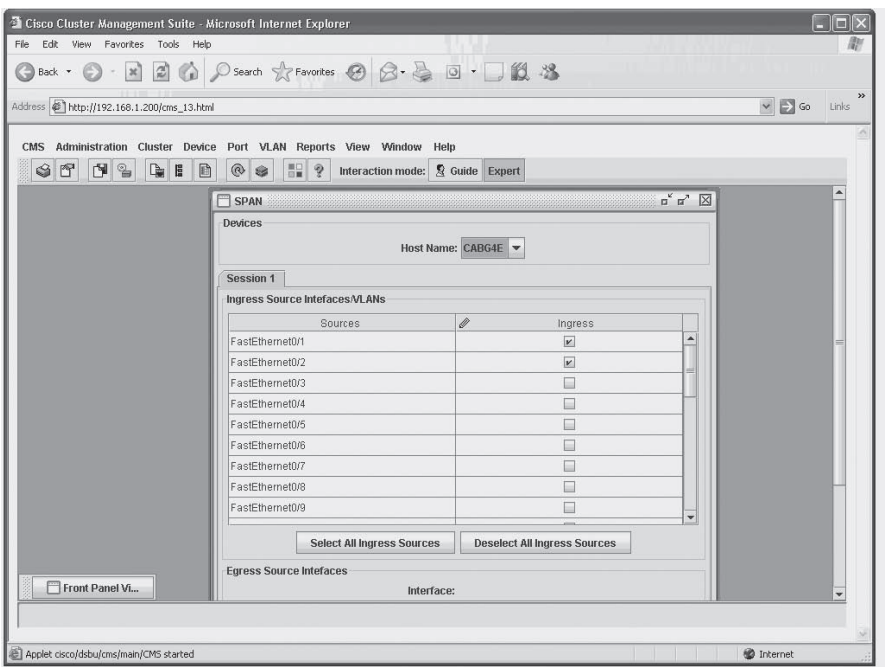


Figura 5-22. Los puertos conmutados individuales pueden seleccionarse para su monitoreo en tiempo real.

desde un NMM, que generalmente son PC o estaciones de trabajo UNIX. Es útil contar con este tipo de información de una red conmutada para que los administradores de red anticipen y resuelvan problemas en las redes. Sin la herramienta SPAN, la administración de los puertos de red en las redes conmutadas requerirían más tiempo y esfuerzo.

Controles para inundación/puertos de red

Una *inundación* (*flooding*) se presenta cuando el tráfico recibido en un puerto conmutado se transfiere a todos los demás puertos. Los conmutadores se inundan cuando reciben mensajes que tienen direcciones de destino desconocidas. Es necesaria la inundación en las redes conmutadas porque dependen de las direcciones MAC de los dispositivos físicos y no de las direcciones IP lógicas, como en el caso de los enrutadores. Si no existiera la inundación en las redes conmutadas, la primera red podría eliminar un mensaje, al no saber acerca de su dirección MAC de destino, y terminar de esta forma la transmisión.

Sin embargo, es necesario que existan controles para asegurar que el conmutador no se ahogue por efecto de una saturación de mensajes de inundación. La posibilidad de que se presente una inundación empeora por el hecho de que los mensajes son transferidos por un conmutador a todas las VLAN en que tiene membresía (con frecuencia, los conmutadores son multi-VLAN). En la figura 5-23 se muestra la página Flooding Control. La ventana de diálogo Flooding Control se ubica en el menú Ports.

El control de la inundación bloquea el envío del tráfico de inundación innecesario utilizando una de las técnicas siguientes:

- ▼ Envío de todos los mensajes de inundación a través de un solo puerto (el *puerto de red*) de tal forma que sólo se inunde ese puerto.
- ■ Habilitación de los *umbrales de tormenta difundida* para limitar cuántos mensajes inundados aceptará un puerto.
- ▲ Bloqueo del envío de mensajes unidirigidos (uno a uno) y de emisión (uno a todos), que se muestran en el campo *Recive Unknown MACs*.

Administración IP

Para que un conmutador funcione en una red, debe tener varias direcciones IP asignadas. La ventana IP Addresses que se muestra en la figura 5-24 se utiliza para administrar y actualizar la información IP. Se puede acceder a esta ventana seleccionando IP Addresses del menú Administration. Esta ventana contiene dos fichas: Interface Configuration y Device Configuration. Las tres direcciones IP obligadas son las siguientes:

- ▼ **Dirección IP del host** Es una dirección de 32 bits asignada a los hosts que utilizan TCP/IP, y están escritos como cuatro octetos separados por puntos (por ejemplo, 209.98.86.52).
- ■ **Máscara de subred IP** Es una máscara que cubre una dirección IP completa que sirve para indicar los bits de la dirección IP completa que se utiliza para dirigirse a la subred local; a menudo se llama simplemente, *máscara*. La máscara es siempre una parte del lado izquierdo de la dirección IP total (por ejemplo, 255.255.255.248).

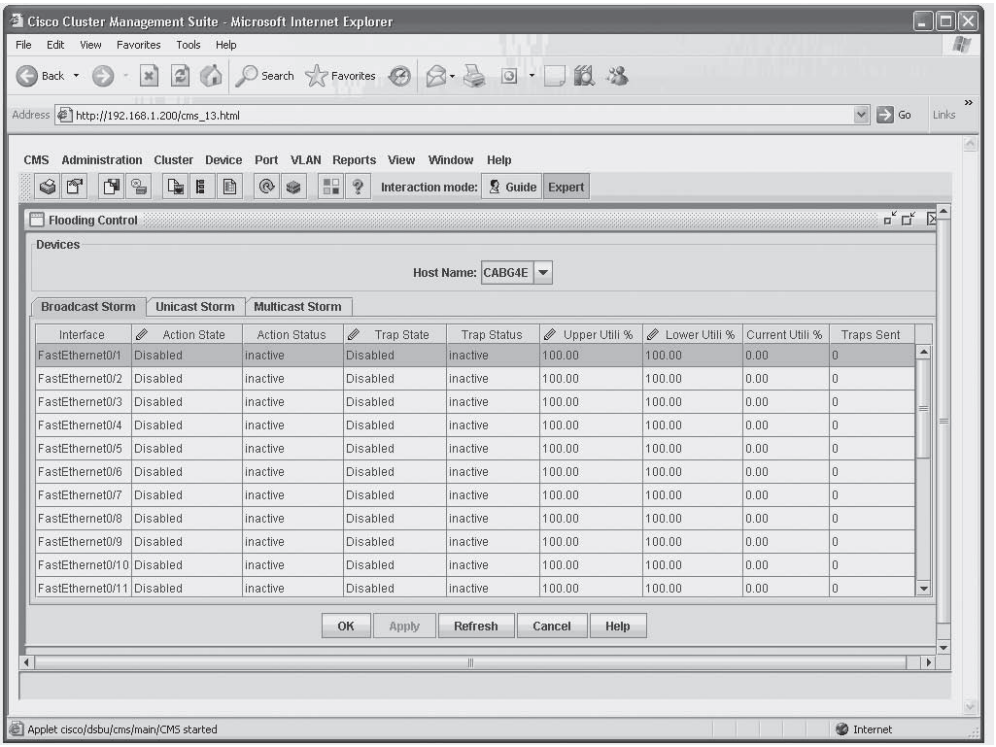


Figura 5-23. En las redes conmutadas, los mensajes inundados y ampliamente dirigidos pueden estar limitados.

- **Compuerta predeterminada** El conmutador envía tráfico a una dirección IP desconocida a través de la compuerta predeterminada. Cuando un mensaje se envía fuera de la red local, éste se enruta a través de la compuerta predeterminada, que tiene una o más direcciones externas. La dirección de la compuerta predeterminada es a veces un proveedor de servicios de Internet (ISP).

Configuración SNMP

SNMP (Simple Network Management Protocol, protocolo simple de administración de la red) es una aplicación IP que se utiliza para administrar y reparar fallas de los dispositivos de red desde la estación de administración de la red (NMS). El SNMP es un estándar industrial, no un protocolo propietario de Cisco. La interfaz que se muestra en la figura 5-25 es, desde luego, de Cisco, pero los parámetros que se configuran a través de esta ventana posibilitan la creación de información SNMP generalizada que puede utilizarse en cualquier producto SNMP de software, no sólo de Cisco. Se accede a esta ventana seleccionando SNMP en el menú Administration.

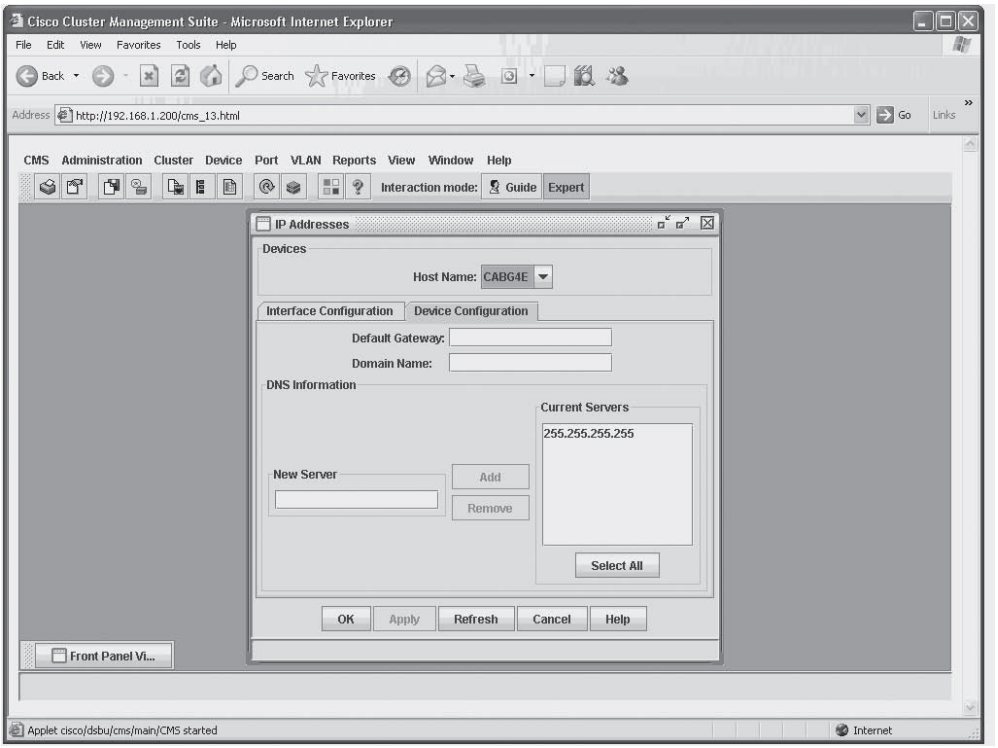


Figura 5-24. La ventana IP Addresses se utiliza para cambiar la información de la dirección IP.

Tiene la alternativa de no habilitar la administración SNMP para el conmutador. La deshabilitación del SNMP evita que las aplicaciones de administración de redes basadas en el SNMP puedan monitorearse o reconfigurar el conmutador.

El SNMP trabaja por medio de la configuración de *agentes* en un dispositivo. Estos agentes son pequeño programas de software que observan la actividad en el conmutador y envían alertas llamadas *trampas* al NMS, informándole de eventos que tengan importancia. La administración de las trampas se encuentra en la ficha Trap Managers.

Las cadenas comunitarias están habilitadas en la ficha Community Strings. Una *cadena comunitaria* es un texto entrelazado que actúa como un tipo de contraseña de grupo que se utiliza para autentificar los mensajes que se envían entre el NMS y los dispositivos que éste administra. Las cadenas comunitarias se envían en cada paquete que circula entre el administrador y el agente SNMP. Consulte el capítulo 13 para encontrar información acerca de los diferentes productos de Cisco que incorporan la funcionalidad SNMP.

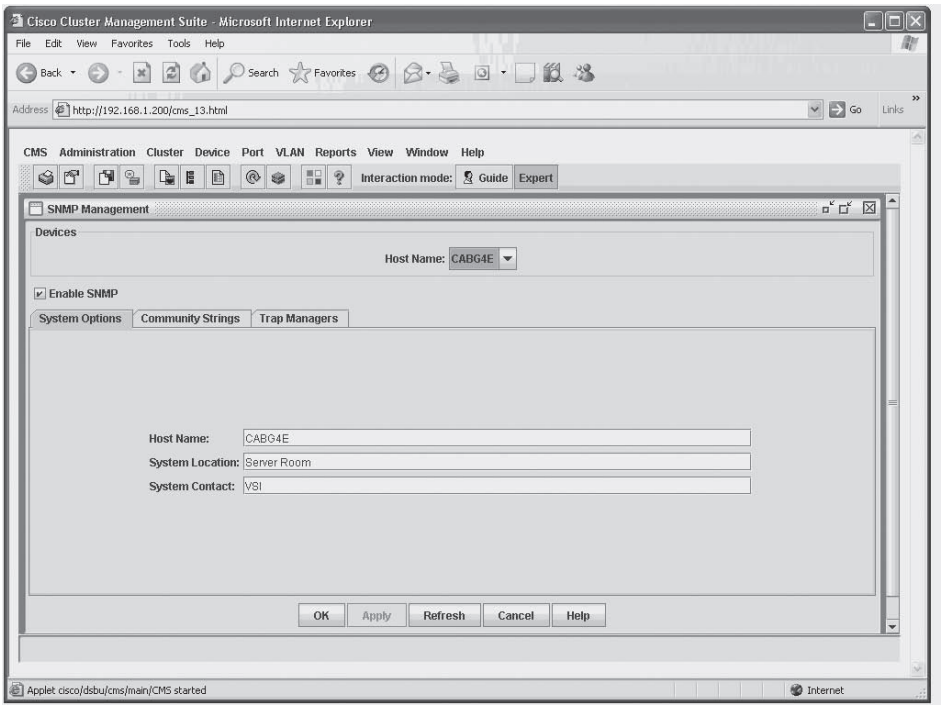


Figura 5-25. Esta ventana se utiliza para configurar la administración SNMP en un conmutador Cisco.

Tabla ARP

ARP (Address Resolution Protocol, protocolo de resolución de direcciones), que es un protocolo estándar en la industria para la asignación de direcciones IP a direcciones MAC. La traducción de direcciones es necesaria, porque cuando un mensaje llega a su LAN de destino, ésta debe convertir la dirección IP lógica a la dirección MAC física para conocer con qué dispositivo de host físico comunicarse. En las tablas ARP que residen dentro de los conmutadores Cisco, la dirección IP se encuentra en la columna izquierda y la dirección MAC con la que está asociada está en el centro de la columna. En la figura 5-26 se muestra la ventana de configuración del ARP.

Las direcciones se agregan dinámicamente a la tabla ARP a medida que los mensajes pasan por el conmutador. Para evitar que la tabla crezca indefinidamente, el campo ARP Cache Timeout Value (ubicado debajo de la ficha ARP Cache Timeout) limita el tiempo que pueden permanecer los valores en la tabla antes de que se eliminen. La tabla ARP se deshace de las direcciones no utilizadas durante ese periodo específico, con *excepción* de las que se agregaron a la tabla manualmente como parámetros ARP permanentes o estáticos. El periodo de envejecimiento predeterminado se fija en 14 400 segundos (cuatro horas).

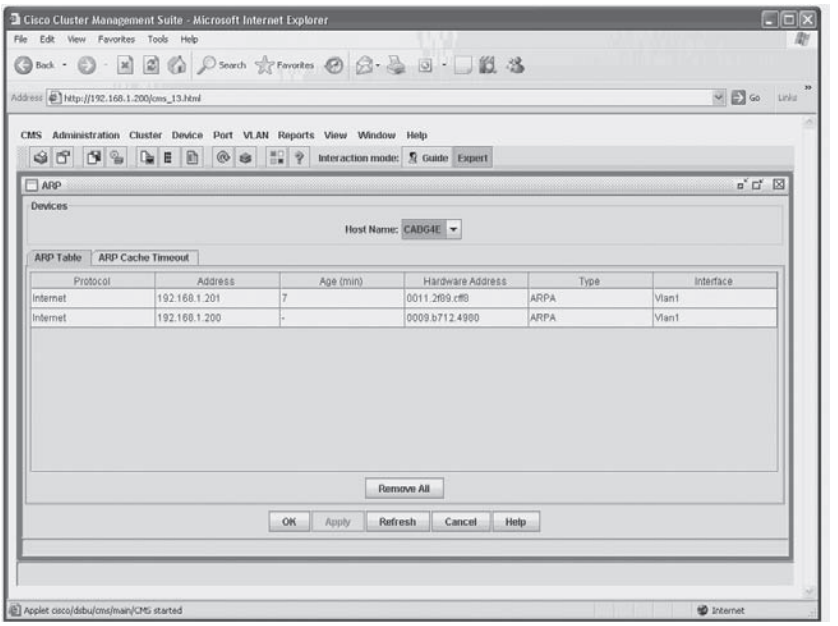


Figura 5-26. En los conmutadores, las tablas ARP determinan los nombres de las VLAN pero no los de las LAN.

Administración de direcciones

Los conmutadores usan la tabla de direcciones (también llamada tabla de administración de direcciones) para decidir adónde enviar los mensajes entrantes. La tabla de direcciones asocia una lista de direcciones MAC con puertos específicos en el conmutador. A diferencia de las direcciones IP, las direcciones MAC son un tipo de números de serie de las redes que identifican los dispositivos físicos de las redes (por lo general, la tarjeta de interfaz de red). Las tablas de direcciones son la parte central de la arquitectura de las redes conmutadas, porque éstas guían los mensajes a sus destinos. Las direcciones MAC funcionan en las redes conmutadas de la misma forma que las direcciones IP lo hacen en las redes basadas en enrutadores. Existen tres tipos de tablas de direcciones, que están localizadas en fichas individuales, como se muestra en la figura 5-27.

La ventana se puede abrir seleccionando MAC Addresses del menú Administration. Las tablas son las siguientes:

- **Tabla de direcciones dinámicas (ficha Dynamic Address)** La construye el conmutador asociando los números de puerto de los mensajes entrantes con las direcciones MAC de origen.
- **Tabla de direcciones seguras (ficha Secure Address)** Una dirección segura sólo tiene un puerto de destino; se ingresan en forma manual y no envejecen.

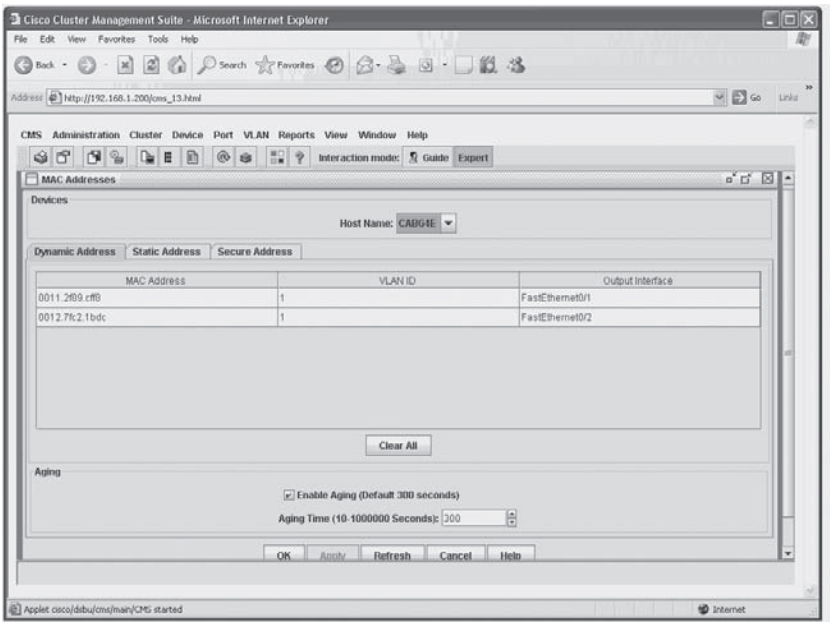


Figura 5-27. La tabla de direcciones es la clave para saber cómo funcionan las redes conmutadas.

- **Tabla de direcciones estáticas (ficha Static Address)** Es como una dirección segura en el sentido de que pueden ingresarse en forma manual y no envejecen, pero una dirección estática se aplica a todo un conmutador en lugar de aplicarse solamente a un solo puerto.

Casi todos los puertos en las redes conmutadas utilizan el direccionamiento dinámico; de esta forma, la red puede ayudar a funcionar sin necesidad de la intervención humana. El direccionamiento estático se utiliza para el agrupamiento de puertos, mientras que el seguro se utiliza para proteger recursos de red y datos de propietario valiosos.

Seguridad de los puertos

Un *puerto seguro* se establece al crear una lista que tenga una o más direcciones MAC de origen y que pueda enviar tráfico a dicho puerto. En este sentido, un puerto seguro es una forma de puerto de acceso estático. La seguridad de los puertos no debe confundirse con las alertas SNMP y otras aplicaciones de seguridad. La seguridad de los puertos trabaja restringiéndole a un puerto, el acceso a enlaces nombrados explícitamente. A menudo esto se lleva a cabo por razones de desempeño y de seguridad de los datos. En la figura 5-28 se muestra la ventana Port Security. Se accede a esta ventana seleccionando Port Security del menú Port.

Las ventajas de asegurar un puerto son que los dispositivos desconocidos no se pueden conectar al puerto sin su conocimiento. Es también una forma muy buena de dedicar el ancho de banda del puerto asignando el tamaño de la tabla de direcciones del puerto a 1, con lo que se pone a disposición de ese dispositivo todo el ancho de banda del puerto. Se asegura un puerto seleccionando la casilla de verificación de la columna Security, además de uno o ambos campos Trap and Shutdown. La seguridad de los puertos no puede habilitarse en un puerto multi-VLAN.

Cisco Group Multicast Protocol (protocolo de transmisión múltiple de grupo de Cisco)

El protocolo de transmisión múltiple de grupo de Cisco (CGMP) es un protocolo de propietario de Cisco que se utiliza para limitar el envío de paquetes de transmisión múltiple (uno a muchos) IP en una red. Por ejemplo, un conmutador deberá formarse para recibir mensajes de transmisión múltiple anunciando nuevas direcciones MAC de redes fuera de la intranet. El CGMP es como un servicio de procesamiento de suscripciones en que los hosts se inscriben en un grupo que recibe cierto tipo de mensajes de transmisión múltiple. Se accede a la ventana CGMP que se muestra en la figura 5-29 seleccionando CGMP del menú Devices.

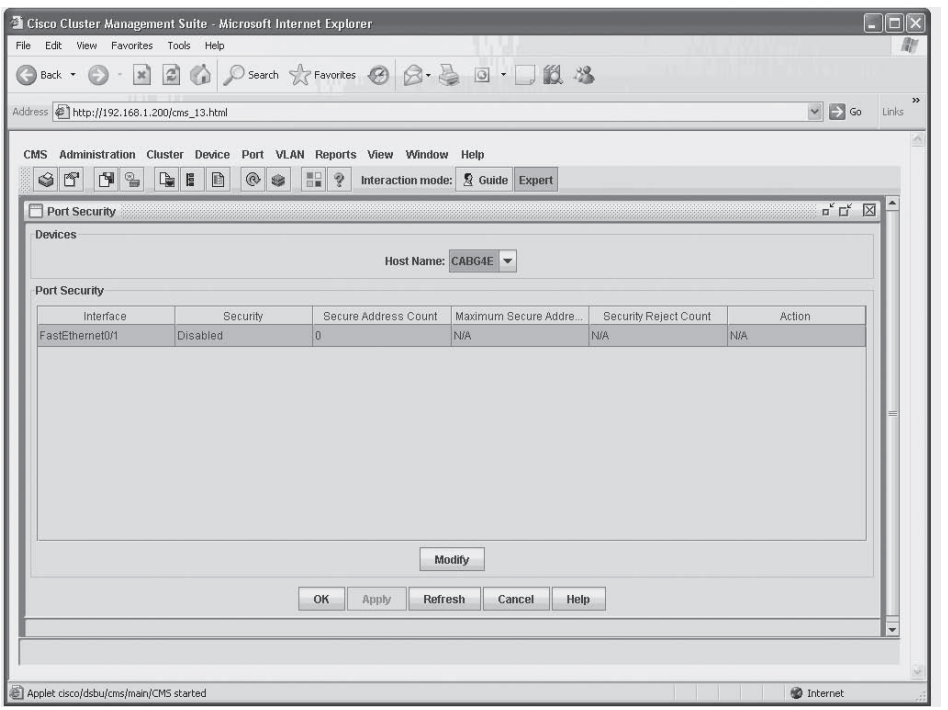


Figura 5-28. Un puerto seguro sólo recibe tráfico de estaciones definidas por el usuario.

Los hosts generan mensajes *de unión* para unirse a un grupo de transmisión múltiple y *dejan* que los mensajes se eliminen. De la misma forma que casi todos los protocolos en que se construyen tablas, el CGMP elimina las suscripciones no utilizadas para limitar el tamaño de la tabla. El parámetro Router Hold Time (fijado en 300 segundos en el ejemplo de la figura 5-29) elimina una entrada después de un periodo especificado por el usuario.

La tabla CGMP se mantiene en un enrutador. Por tanto, para que el CGMP funcione, un conmutador debe contar con una conexión a un enrutador que esté operando el CGMP y el IGMP (Internet Group Management Protocol, protocolo de administración de grupos de Internet). El IGMP es utilizado por los hosts IP para reportar sus membresías de grupo de transmisión múltiple a un enrutador de transmisión múltiple adyacente. Cuando el enrutador recibe una solicitud IGMP (de abandonar o de unirse) por parte de un cliente, envía esta información al conmutador como un paquete CGMP. El conmutador utiliza esta información para modificar su comportamiento de envío.

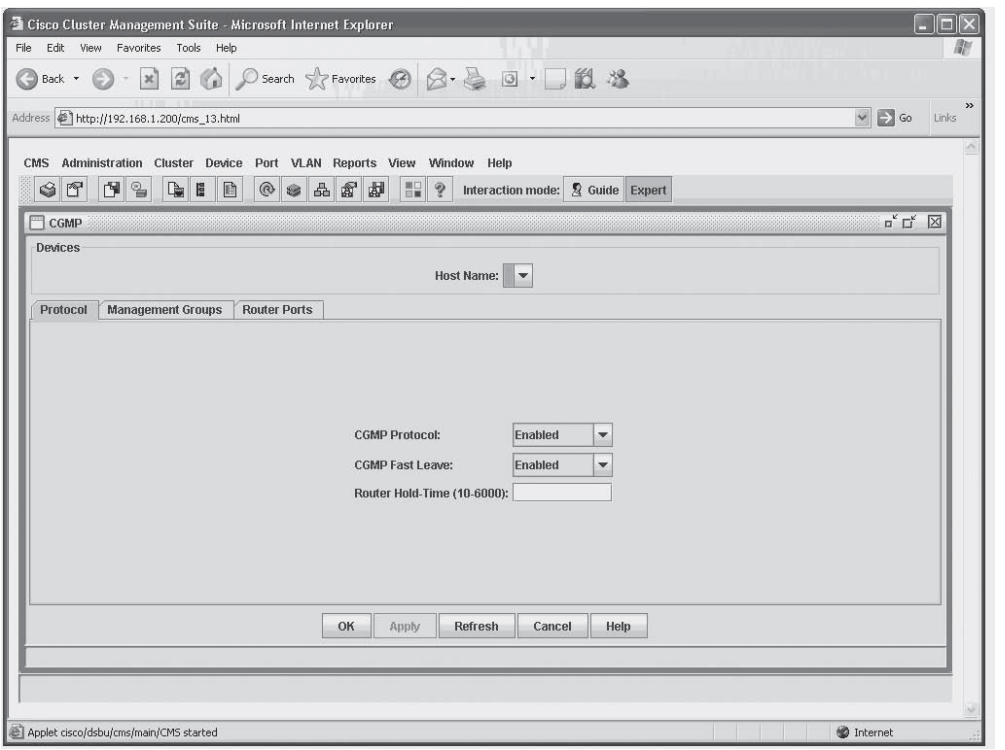


Figura 5-29. El CGMP se utiliza para inscribir puertos del conmutador en grupos multidirigidos.

Spanning-Tree Protocol (protocolo de árbol expandido)

El protocolo de árbol expandido (STP) es una técnica estándar en la industria para prevenir la aparición de bucles de retorno en las redes conmutadas. Las redes conmutadas utilizan direcciones MAC en lugar de las direcciones lógicas IP. Trabajan enviando un mensaje a cualquier conmutador que contenga la dirección MAC deseada. Sin el STP, las redes conmutadas son susceptibles de usar trayectorias que vuelvan atrás hacia el conmutador que envió el mensaje (provocando una entrega lenta y generando tráfico innecesario).

STP trabaja identificando trayectorias redundantes y bloqueando al menos una de ellas. Se accede a la ventana Spanning-Tree Protocol seleccionando el STP desde el menú Device. Esta ventana contiene siete fichas que se utilizan para administrar los detalles del STP. Spanning-Tree Protocol se muestra en la figura 5-30 y se utiliza para habilitar un conmutador para que pueda utilizar el STP y para definir un conmutador raíz para cada VLAN. Contar con un conmutador raíz para una VLAN ayuda al algoritmo STP a decidir qué trayectorias bloquear o no bloquear. STP utiliza un sistema de asignación de *costo a cada ruta*, no como los

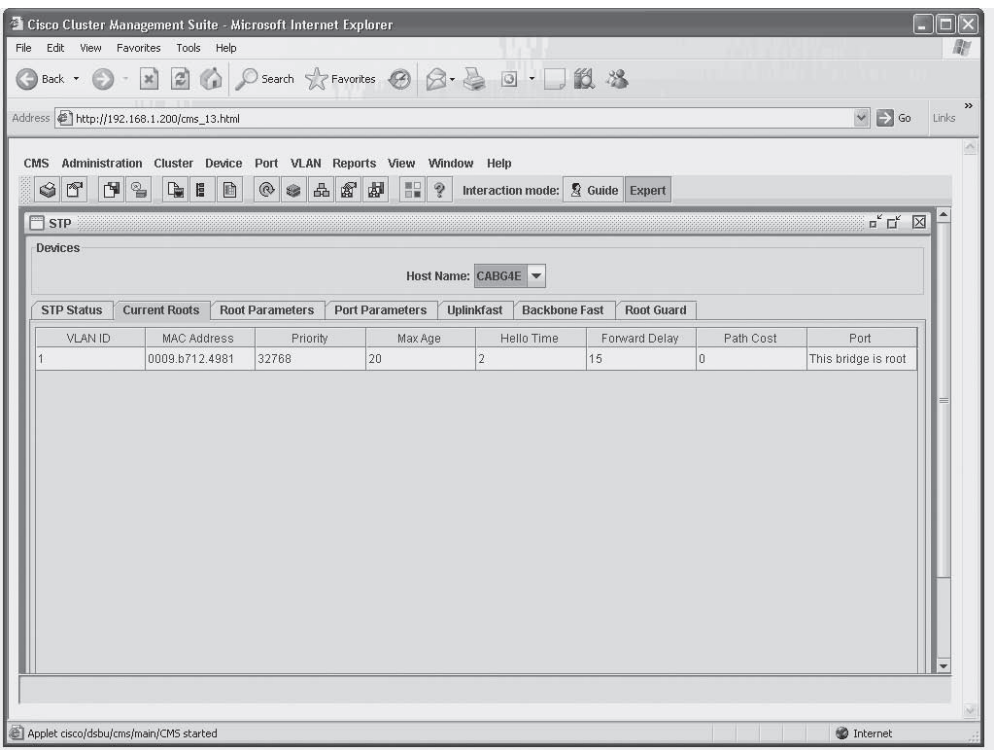


Figura 5-30. El STP evita la proliferación de trayectorias cerradas en las redes conmutadas.

protocolos de enrutamiento que se analizan en el capítulo 12. Un costo de ruta bajo, significa una velocidad más elevada (por ejemplo, un costo de trayectoria de 100 por 10 Mbps contra una de 4 por 1 Gbps). El parámetro Hello Time establece el número de segundos entre mensajes STP. El parámetro Max Age establece cuánto tiempo puede esperar el conmutador entre mensajes STP antes de que se reconfigure el STP por sí solo.

Membresía VLAN

La membresía VLAN es sólo cuestión de asignar un puerto del conmutador a una o más LAN virtuales. El número máximo de VLAN al que un puerto puede pertenecer está en función del modelo del conmutador. El conmutador de ejemplo que se muestra en la figura 5-31 es un Catalyst 2950-24 de Cisco, que soporta hasta 64 VLAN por puerto. Los modos de membresía de las VLAN son los siguientes:

- Modo de membresía VLAN de acceso estático.
- Modo de membresía multi-VLAN.

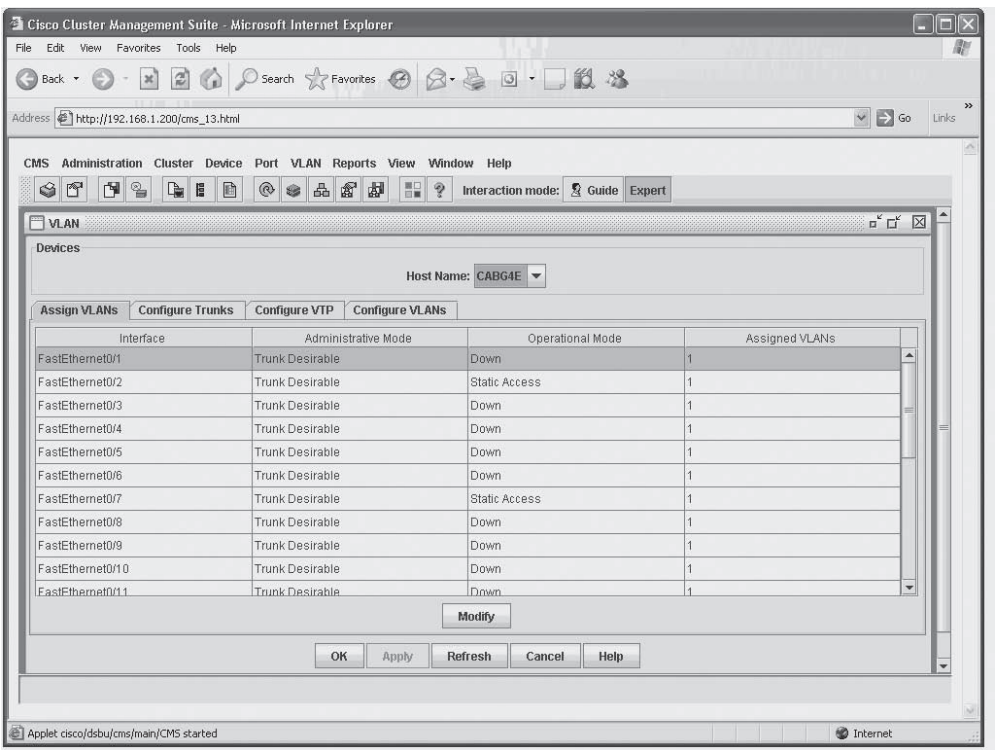


Figura 5-31. Un puerto puede pertenecer a una o más VLAN y utilizar cualquiera de los cuatro modos de membresía.

- ■ Modo de membresía VLAN de acceso dinámico.
- ▲ Modo de membresía VLAN de troncal ISL.

ISL, Inter-Switch Link (vínculo entre conmutadores) es un protocolo propietario de Cisco para la interconexión de múltiples conmutadores y el mantenimiento de información acerca de las VLAN a medida que el tráfico circula entre ellas. ISL proporciona capacidades VLAN mientras que mantiene un alto desempeño en vínculos Fast Ethernet en modo full-duplex y half-duplex.

Se requiere un grupo especial de características de software del IOS en un conmutador, para que éste pueda trabajar en modos VLAN avanzados el multi-VLAN y el VLAN de acceso dinámico.

Administración del VTP

El VLAN Trunk Protocol (VTP, protocolo de troncales VLAN) permite que los administradores de red hagan cambios de configuración en un solo conmutador y comuniquen automáticamente dichos cambios a todos los demás conmutadores de la red. La configuración central elimina un gran número de problemas, como nombres VLAN duplicados, especificaciones incorrectas acerca del tipo de VLAN y violaciones de seguridad. El VTP envía anuncios a través de la red conmutada como una forma de mantener las membresías de troncal VTP y transmitir otras modificaciones en la configuración del VTP. La configuración del VTP se mantiene como una base de datos VLAN almacenada en la NVRAM de los conmutadores miembros. Un conmutador puede estar en cualquiera de los tres modos del VTP:

- ▼ **Modo VTP cliente** Es un conmutador que se habilita para el VTP; puede enviar anuncios, pero no puede configurar las VLAN.
- ■ **Modo VTP transparente** Es un conmutador que está deshabilitado para su uso con el VTP; no puede enviar sus propios anuncios, pero puede recibirlos y enviarlos hacia y desde otros conmutadores.
- ▲ **Modo de servidor VTP** Es un conmutador que está habilitado para VTP; puede enviar anuncios y configurar las VLAN.

Como se muestra en la figura 5-32, la pantalla VTP Management despliega la información sobre el estado del VTP en la parte superior e ingresa las modificaciones en los parámetros de la configuración en la parte inferior.

El ISL trabaja encapsulando los marcos que circulan a través de un conmutador con un encabezado ISL, permitiendo que otros conmutadores en la troncal se filtren a través de los mensajes encapsulados ISL como “nativos” de esa troncal. El formato etiquetado IEEE 802.1Q, un estándar abierto que no es propietario de Cisco, soporta tráfico etiquetado o no etiquetado simultáneamente en un puerto del conmutador.

Configuración del VMPS

VLAN Membership Policy Server (VMPS, servidor de directivas de membresía VLAN) asigna dinámicamente puertos del conmutador a VLAN con base en la dirección MAC del dispositivo conectado al puerto. Cuando un host se mueve desde un puerto en un conmutador de la red a otro puerto en otro conmutador de la red, se asigna automáticamente a la VLAN apropiada. Un VMPS mantiene una base de datos que compara las direcciones MAC

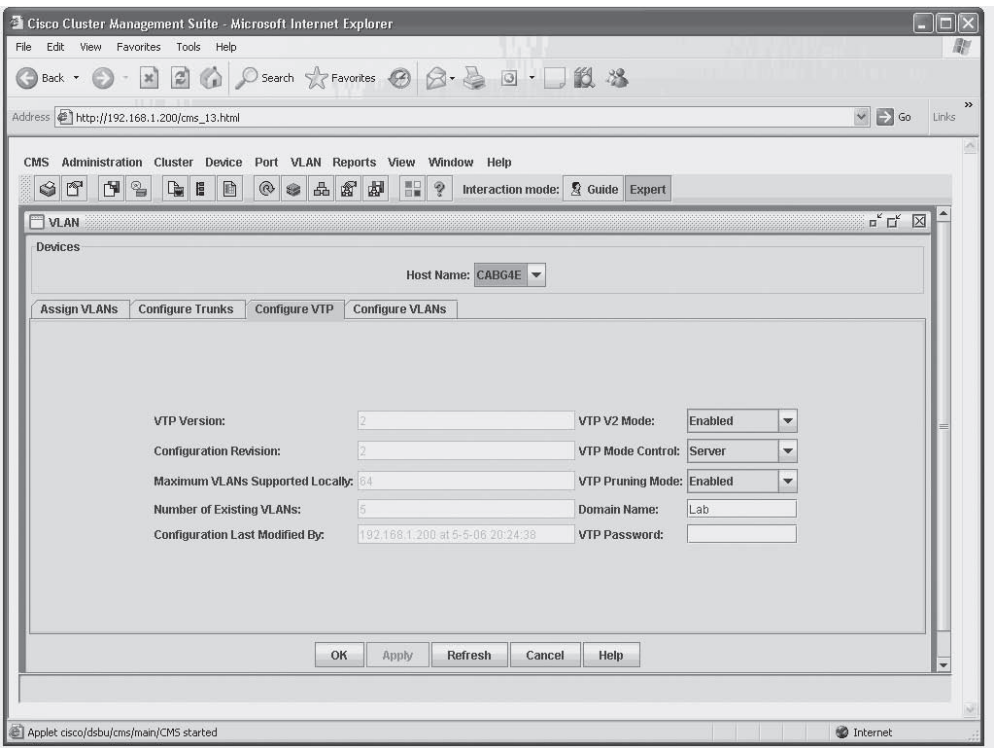


Figura 5-32. El VTP administra centralmente las configuraciones de las redes conmutadas.

de los puertos habilitados en el VMPS con las VLAN. Dicha base de datos puede descargarse del servidor utilizando el Trivial File Transfer Protocol (TFTP, protocolo de transferencia trivial de archivos).

El VMPS es útil para las empresas en que los usuarios se mueven mucho entre diferentes puntos y utilizan sus computadoras laptop para acceder a la intranet desde donde estén. La página de configuración del VMPS (figura 5-33) se utiliza para configurar el servidor VMPS, agregar o quitar VLAN y configurar una VLAN principal.

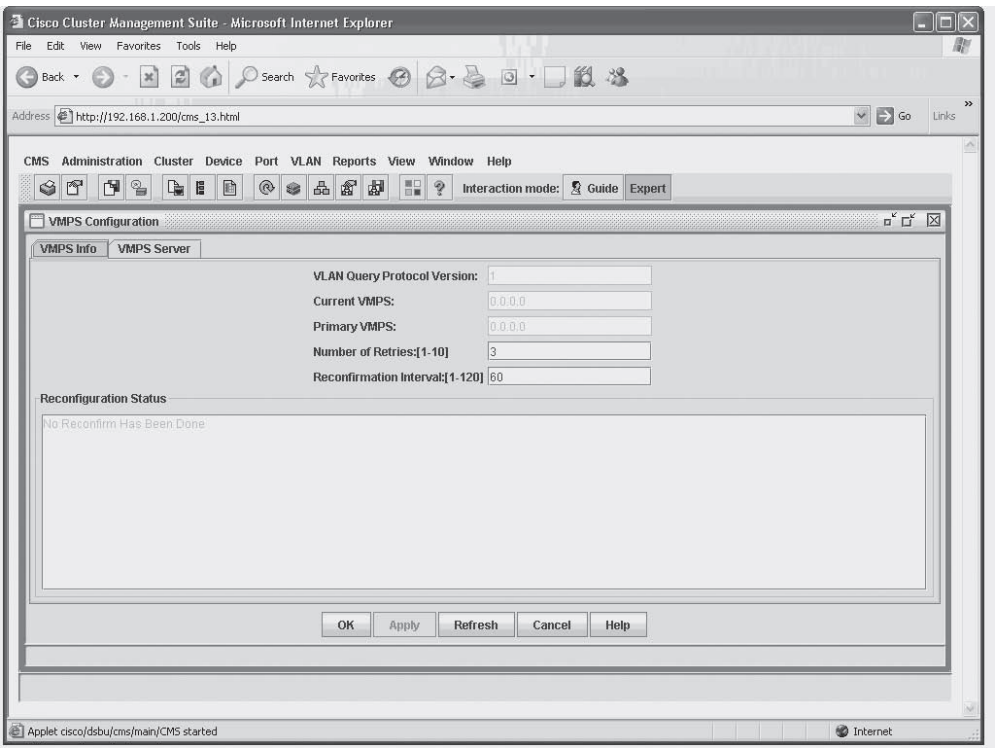


Figura 5-33. El VPMS es una forma automática de asignar los puertos del conmutador a las VLAN.

Los conmutadores representan una manera importante de proporcionar conectividad a la red de una organización. Éstos no sólo conectan dispositivos a la red, también ofrecen una etapa intermedia importante entre la PC y la interconexión. Además de un gran número de opciones de conmutadores para compañías grandes y pequeñas, Cisco también proporciona una herramienta poderosa de administración en su software CMS.

CAPÍTULO 6

Panorama general de la seguridad

El concepto de seguridad en redes podría parecer de alguna forma uno o varios objetivos que no se quedan quietos. Cuando hablamos de "seguridad", sabemos lo que *queremos*, pero describirlo y hacer que se cumpla pueden ser cosas muy diferentes. La seguridad de la red tiene un conflicto natural con la conectividad de las redes. A medida que un sistema autónomo es más abierto, mayor riesgo tiene. Esto, a su vez, requiere de la aplicación de un mayor esfuerzo en las tareas concernientes a hacer que las tareas relacionadas con el cumplimiento de la seguridad se lleven a cabo.

Arriba de todo esto, agregue las restricciones de presupuesto del departamento (y los recortes de personal que muchas compañías han experimentado en años recientes), y aun soluciones razonables en cuanto a seguridad parecerían imposibles de alcanzar. Tres tendencias han provocado el aumento del presupuesto que debe destinar el departamento de tecnología de la información al tema de la seguridad:

- ▼ Las interconexiones se están haciendo cada vez más grandes y complejas.
- ■ Constantemente aparecen nuevas amenazas.
- ▲ El sistema típico de seguridad en las redes, no suele ser un sistema, sino un parche formado con herramientas del fabricante del equipo (¿le suena familiar?).

La seguridad en las redes es una consideración tan amplia que aun las consolas de administración de redes despiertan preocupaciones. Algunos, por una buena razón, se preocupan por saber si la infraestructura del SNMP es en sí lo suficientemente segura. Después de todo, robar la cadena comunitaria del SNMP le daría a un intruso un mapa completo de la configuración de toda una interconexión, y a menos que haya vivido en una cueva, sabe acerca de la expansión, en varias formas, de los virus de computadora: bombas por correo electrónico, applets de Java que funcionan como caballo de Troya, ataques de negación del servicio (DoS, Denial-of-Service) y otras nuevas amenazas preocupantes respecto a la seguridad de las computadoras. Es suficiente mencionar que se invierte gran cantidad de tiempo, dinero y esfuerzo en el rubro de la seguridad en redes.

NOTA SNMP son las siglas de Simple Network Management Protocol (protocolo simple de administración de la red) y, como lo habrá deducido, se usa para administrar la red como una forma de reunir información de varios dispositivos. Existen tres versiones, llamadas SNMPv1, v2 y v3. Las versiones 1 y 2 utilizaron cadenas comunitarias, un nombre "secreto" que se utilizaba para permitir o negar el acceso a la información del SNMP. Esto se enviaba en texto normal y se ponía en peligro con facilidad. El SNMPv3 finalmente proporcionó un mecanismo de autentificación junto con la capacidad para codificar información del SNMP, de tal forma que la información no pudiera leerse durante la transmisión.

En el capítulo 7, hablaremos acerca de los productos de Cisco para el acceso a Internet y la seguridad. Como avance, el enfoque será principalmente en la manera en que los firewalls, y aún los enrutadores, monitorean el tráfico en la interconexión en el nivel del paquete para proporcionar seguridad. Este tipo de seguridad "de la capa de red" trabaja en la capa OSI que la gente asocia con las direcciones IP.

Pero un segundo tipo de seguridad trabaja en el nivel de la *gente*. Este tipo, llamado *seguridad basada en el usuario*, utiliza contraseñas y otros controles de acceso para autenticar

las identidades de los usuarios antes de permitirles el acceso. Existen dos tipos básicos de seguridad basada en el usuario:

- ▼ Acceso remoto de los usuarios a los servidores, en el que los empleados marcan a sus interconexiones corporativas y los suscriptores marcan a sus proveedores de servicio de Internet (ISP).
- ▲ Acceso del administrador de la red a los dispositivos de la red, en que los técnicos se registran al IOS a través de varios tipos de dispositivos de red para trabajar con ellos.

La seguridad es el tercer sistema principal de control en la interconectividad, junto con los sistemas de administración de la red y los protocolos de enrutamiento. Aunque los tres sistemas de control tienen misiones diferentes, podrá observar un patrón común:

- ▼ **Comandos incrustados** Son comandos de aplicación que se encuentran en el IOS y se utilizan para configurar los dispositivos individuales con el fin de que participen en sistemas más grandes de control de la red.
- ■ **Protocolo de control dedicado** Es un protocolo de comunicaciones que coordina el intercambio de los mensajes necesarios para realizar las tareas de los sistemas de control de la red.
- ▲ **Servidor y consola** Es un servidor que almacena los mensajes y una estación de trabajo que brinda la interfaz humana para que opere el sistema de control de la red.

En la figura 6-1 se muestra la arquitectura común que comparten los sistemas de control de la red. Si revisa la figura, observará dos nombres nuevos listados junto al SNMP (TACACS

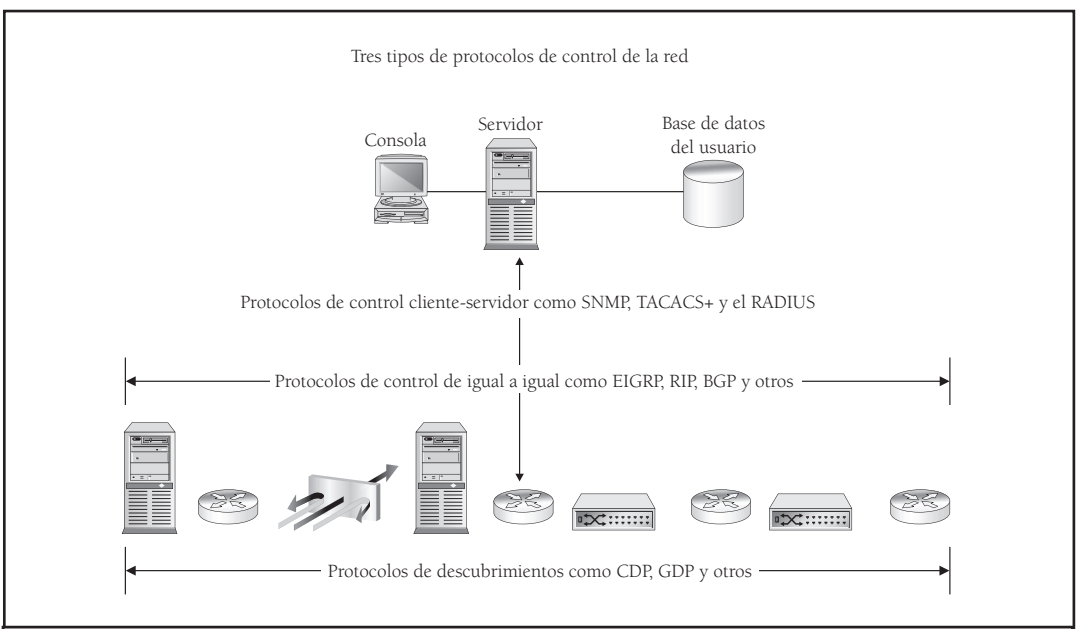


Figura 6-1. Los sistemas de control de interconexión, incluidos los de seguridad, comparten ciertas características.

y RADIUS). Son los protocolos que se utilizan para la seguridad, no para la administración, como en el SNMP, pero suelen trabajar de manera similar, en el sentido de que son protocolos utilizados para comunicar información a través de una red. En el caso del SNMP, los datos recolectados provienen de los dispositivos de red, se almacenan en una base de datos central, y se utiliza una consola para configurar los dispositivos desde una estación de trabajo central de administración. Los sistemas de administración de la red y los de seguridad difieren en lo que hacen, pero son similares en la forma que utilizan una red para comunicarse.

El tercer sistema de control de interconexión, los protocolos de enrutamiento, difiere significativamente. Este sistema no utiliza servidores, porque la información (las tablas de enrutamiento) es transitoria y no necesita almacenarse en disco. Además, no se utilizan consolas porque trabajan por sí mismas.

PANORAMA GENERAL DE LA SEGURIDAD DE LAS REDES

Existen dos tipos de seguridad en las redes acerca de las que hablaremos aquí. Un tipo es impuesto como proceso tras bambalinas y no es visible a los usuarios; el otro sí es visible:

- **Seguridad basada en el tráfico** Controla las conexiones solicitadas por una aplicación de red, como un navegador Web o una descarga FTP.
- **Seguridad basada en el usuario** Controla la admisión de personas a los sistemas para arrancar aplicaciones una vez que están dentro, generalmente mediante el nombre del usuario y su contraseña.

Un tipo de seguridad basada en el tráfico consiste en el uso de firewalls para proteger sistemas autónomos al vigilar el tráfico de hosts no confiables. Otro tipo de seguridad basada en el tráfico son las listas de acceso al enrutador, utilizadas para restringir el tráfico y los recursos dentro de un sistema autónomo. La seguridad basada en el usuario tiene que ver con la gente, no con los hosts. Éste es el tipo de seguridad con la que todos estamos familiarizados (seguridad basada en el acceso, que le solicita un nombre de usuario y una contraseña).

Los dos tipos de seguridad se complementan entre sí, a pesar de que trabajan en diferentes niveles. La seguridad basada en el tráfico se activa cuando hace clic sobre un botón en un navegador Web, teclea un comando en la pantalla FTP o utiliza algún otro comando de aplicación para generar el tráfico de la red. La seguridad basada en el usuario, por otro lado, se prueba a sí misma cuando una persona trata de acceder a una red, un dispositivo o al servicio ofrecido en un dispositivo.

Seguridad basada en el tráfico

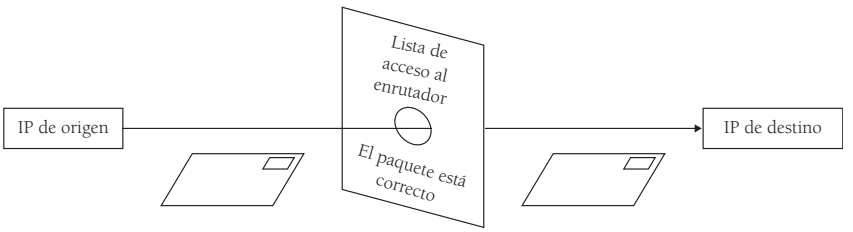
La seguridad basada en el tráfico se implementa en una interconexión de Cisco utilizando listas de acceso a firewalls o enrutadores. Este tipo de seguridad (conocerá más al respecto en el capítulo 7) se concentra principalmente en las direcciones IP de origen y destino, en los números de puertos de la aplicación y en otra información en el nivel del paquete que puede utilizarse para restringir y controlar las conexiones de red.

Hasta hace poco, los firewalls se concentraban estrictamente en la protección contra intrusos externos al sistema autónomo. Sin embargo, en la actualidad se están utilizando

en las tiendas más sofisticadas para restringir el acceso a los bienes delicados de adentro. Las listas de acceso han sido tradicionalmente las herramientas utilizadas para reforzar la seguridad intramuros.

Seguridad basada en el tráfico mediante listas de acceso

Los enrutadores pueden configurarse para reforzar la seguridad en forma muy parecida a los firewalls. Todos los enrutadores pueden configurarse con listas de acceso y pueden utilizarse para controlar qué tráfico puede entrar y salir por las interfaces de red del enrutador. Lo que hace exactamente una lista de acceso depende de la manera en que el administrador configuró la red.

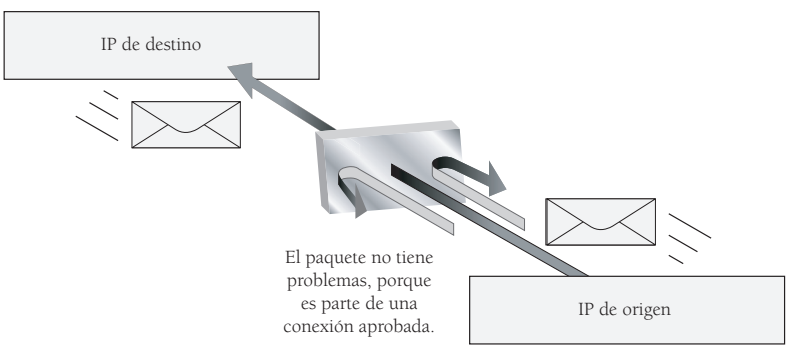


Las listas de acceso se utilizan para mejorar el desempeño de la red, separando el tráfico en su área de origen, pero es más común utilizar listas de acceso para "analizar" el tráfico e implementar restricciones rudimentarias tipo firewall en el tráfico de la red.

Seguridad de firewall basada en el tráfico

Los firewalls para filtrar paquetes son básicamente enrutadores fortalecidos que analizan procesos de acuerdo con estrictas reglas de administración de tráfico. Utilizan todo tipo de tácticas para mejorar la seguridad: traducción de direcciones para ocultar la topología interna de la red de los intrusos; inspección de la capa de aplicación para asegurarse que sólo se estén ejecutando los servicios permitidos; contadores de alto/bajo que vigilen los picos en determinados tipos de paquetes para ahuyentar a ciertos ataques de negación de servicio (DoS), como SYNflood y FINwait.

Los firewalls crean intencionalmente un cuello de botella en el perímetro del sistema autónomo. Conforme el tráfico circula, el firewall inspecciona los paquetes que entran y salen de las redes conectadas a sus interfaces.



Los firewalls leen las direcciones host y los números de puerto de origen y destino (por ejemplo, puerto 80 para HTTP), y establecen un contexto para cada conexión permitida. El contexto viene en la forma de una sesión, donde los paquetes con cierto par de direcciones y número de puerto, deben pertenecer a una sesión válida. Por ejemplo, si un usuario trata de conectarse al servidor Web para descargar un archivo, el firewall verificará la dirección IP de origen del usuario y el servicio de aplicación que se solicitó antes de dejar que pasen los paquetes. Si el tráfico es permitido, al usuario se le dejará conectarse el servidor Web. Si no, el tráfico se negará y no se permitirá que se lleve a cabo la conexión.

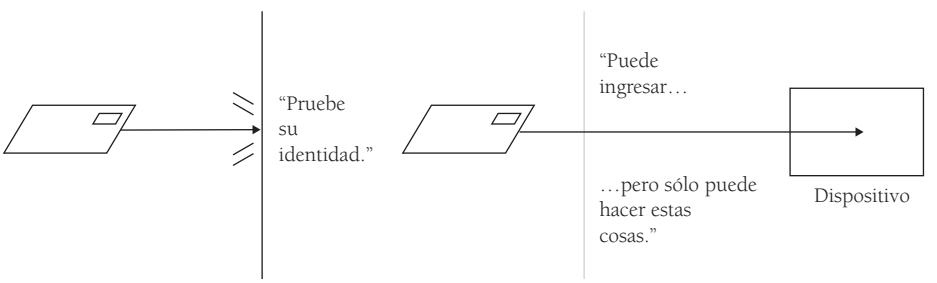
Se debe considerar que la seguridad basada en el tráfico es como las casetas de cobro automáticas que existen en algunas carreteras. Los vehículos se hacen pasar por una compuerta donde un láser lee cada ID electrónica, lo que reduce muy poco la velocidad del tráfico. Una vez que se le autoriza el pase, nadie revisará lo que pudiera traer en la cajuela de su carro.

Seguridad basada en el usuario

La seguridad basada en el usuario trae a la mente una imagen diferente (una compuerta con guardias de seguridad malhumorados parados en sus puestos). El guardia exige saber quién es usted y le exige probar su identidad. Si cumple con los requisitos, podrá entrar. Los sistema de seguridad más sofisticados que se basan en el usuario también cuentan con un guardia que le pregunta qué desea hacer una vez que se encuentre adentro y le asigna una tarjeta codificada para visitante, permitiéndole el acceso a algunas áreas pero a otras no.

Por tanto, la seguridad basada en el usuario se emplea cuando una persona debe registrarse en un host y la seguridad viene en la forma de una solicitud de su número de usuario y contraseña. En las interconexiones, este tipo de seguridad se utiliza para evitar que los agresores entren a dispositivos de red como enrutadores y conmutadores, y para restringir el acceso a dispositivos con información como los servidores.

Sin embargo, a diferencia de los firewalls, a la seguridad basada en el usuario le preocupan tanto los intrusos de adentro como los de afuera. Ese guardia de seguridad en la puerta tiene colegas en el interior para asegurarse de que nadie se dirija al área equivocada. Usted conoce la rutina: existen credenciales para los empleados y para los visitantes, pero las de los empleados le permiten moverse por más lugares.



La autenticación inicio de sesión/contraseña se requiere en general en cada dispositivo de la red y en todos los servidores. Debido a que los mecanismos de seguridad basados en el usuario son de software y no de hardware, pueden utilizarse como se desee dentro de una interconexión, sin que esto tenga un impacto en el desempeño o el presupuesto. La cuestión es qué tantas barreras desea ponerles a los usuarios para que tengan acceso a los diferentes servicios. La seguridad basada en el usuario tiene cuatro aplicaciones principales:

- ▼ Otorgar acceso a los empleados remotos a la interconexión corporativa.
- ■ Otorgar acceso a los empleados en el sitio a hosts protegidos y a servicios dentro de la interconexión.
- ■ Permitir a los administradores de red el acceso a los dispositivos de red.
- ▲ Permitir que los ISP puedan otorgar a sus suscriptores el acceso a sus portales.

Debido a que mucha de la seguridad basada en el usuario incluye conexiones de marcación remota, las tecnologías WAN juegan un papel importante. Los dos dispositivos más importantes de conexiones para la autentificación WAN son los servidores de acceso y los protocolos de marcación.

Servidores de acceso

El ingreso a una interconexión mediante una conexión de marcación telefónica casi siempre se realiza con un servidor de acceso, que es un dispositivo dedicado que contesta las llamadas telefónicas provenientes de individuos remotos que tratan de establecer una conexión con una red. A los *servidores de acceso* también se les denomina *servidores de acceso a la red* o *servidores de comunicaciones*. Su atributo principal es comportarse como un host IP totalmente equipado por un lado, pero como un módem por el otro. En la figura 6-2 se describe el papel que juegan los servidores de acceso en las conexiones de marcación telefónica.

Cuando se conecta a un host de interconexión desde el campus empresarial, por lo general lo hace mediante un cable dedicado de par trenzado que está conectado a un concentrador o un conmutador. Para establecer esa misma conexión desde lejos, utiliza una línea telefónica normal a través de un servidor de acceso (un dispositivo que responde la llamada telefónica y establece una conexión de red). Además de establecer conexiones para usuarios remotos de marcación telefónica, los servidores de acceso también se utilizan para conectar enrutadores remotos.

Seguridad basada en el usuario para conectividad local Cuando enciende su PC e ingresa al sistema en su trabajo, no está utilizando TACACS+ ni RADIUS. Las solicitudes de nombre del usuario y la contraseña vienen de su servidor local. Casi todos los servidores LAN operan sobre plataformas Windows 2000/2003, Linux, UNIX o Novell. Cuentan con subsistemas de seguridad y bases de datos de usuarios propios para autentificar y autorizar a los usuarios. No se utiliza RADIUS debido a que, entre otras cosas, es un protocolo de marcación con contraseña. No se usa TACACS+ porque éste controla el ingreso a los propios dispositivos de red de Cisco (enrutadores, conmutadores y servidores de acceso), además de proporcionar seguridad en la marcación telefónica de manera muy parecida a la de RADIUS.

En este capítulo, el análisis sobre conexiones locales o "en la red" se refieren a los administradores de red que inician sesión en el IOS para trabajar en un dispositivo de red de Cisco.

Seguridad basada en el usuario para conectividad remota Los usuarios de pequeña oficina u oficina en casa se pueden conectar a sus interconexiones empresariales a través de un servidor de acceso, lo que lo convierte, tal vez, en el dispositivo más básico de cualquier red de área local. Los servidores de acceso de extremo inferior son dispositivos discretos de escritorio que nos recuerdan a una PC sin monitor. Cuando marca por teléfono a su ISP para acceder a Internet desde su casa, la llamada es contestada también por un servidor de acceso. Como se imaginará, una sala de cómputo de un ISP está saturada de servidores de acceso de alta densidad montados sobre estantes, para manejar las conexiones que hacen

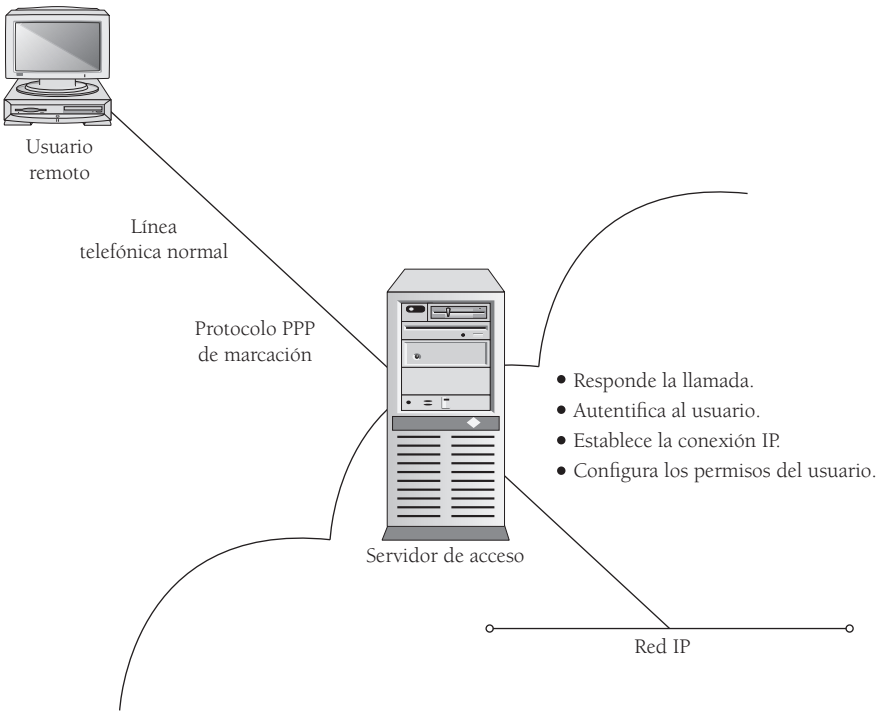


Figura 6-2. Los servidores de acceso están dedicados a soportar conexiones remotas de marcación telefónica.

los miles de suscriptores (como recordatorio, *alta densidad* significa muchos puertos por dispositivo).

Los servidores de acceso son dispositivos inteligentes que manejan otras tareas, además de hacer conexiones de línea. Proporcionan servicios especiales para acomodar configuraciones que se encuentran con frecuencia en las interconexiones corporativas:

- **Servicio de enrutamiento** Proporcionado por servidores de acceso llamados *enrutadores de acceso*, hace parecer como si el usuario que marca residiera en la red del campus. La característica clave de los enrutadores de acceso es el Dial-on-Demand Routing (DDR, enrutamiento de marcación por demanda), que permite enrutar tráfico de una LAN remota a la red principal a través de líneas telefónicas conmutadas de bajo costo.
- **Servicio de terminal** Muchas conexiones WAN aún utilizan protocolos terminales. Por esa razón, casi todos los servidores de acceso soportan protocolos terminales, como TN3270 de IBM, rlogin de UNIX o Local-Area Transport (LAT, transporte de área local) de Digital Equipment. Una PC que opere software de emulación de terminal podría utilizarse para dicha conexión.

- ▲ **Traducción de protocolos** Un usuario remoto puede estar ejecutando un protocolo de terminal virtual y después conectarse a un sistema que ejecuta otro protocolo de terminal virtual. Casi todos los servidores de acceso todavía soportan la traducción de protocolo.

A medida que mejora la infraestructura de cómputo, el uso del servicio de terminales y la traducción de protocolos está decayendo. En contraste, está creciendo la popularidad de los enrutadores de acceso a medida que las oficinas pequeñas construyen LAN y optan por adoptar el DDR por conveniencia y ahorro de recursos.

Protocolos de marcación telefónica

Como ya ha aprendido hasta el momento, existe un protocolo para casi cada tarea principal de interconexión. Hacer que las conexiones de red por marcación telefónica funcionen adecuadamente presenta problemas especiales, porque la mayor parte de la infraestructura de las compañías telefónicas se diseñó para manejar voz y no datos a alta velocidad. Los protocolos de marcación telefónica existen para manejar conexiones punto a punto a través de líneas telefónicas normales:

- ▼ **PPP** Protocolo de punto a punto, es el estándar *de facto* de las conexiones de marcación telefónica remota hacia las redes IP; casi todas las conexiones de marcación telefónica a Internet utilizan PPP. La mayor parte de las conexiones PPP se llevan a cabo sobre líneas asincrónicas, pero un número cada vez más grande se hacen a través de ISDN, en áreas donde se encuentra disponible.
- ■ **SLIP** Serial Line Internet Protocol (protocolo Internet de línea serial) también se utiliza para hacer conexiones conmutadas punto a punto con redes IP desde lugares remotos. SLIP es el predecesor de PPP, pero todavía se utiliza en algunos lugares. También puede encontrar una variante de SLIP llamada CSLIP (Compressed Serial Line Internet Protocol, protocolo comprimido de Internet de línea serial).
- ▲ **ARAP** AppleTalk Remote Access Protocol (protocolo de acceso remoto de AppleTalk) es la herramienta de Apple para la conectividad de marcación telefónica con redes remotas de AppleTalk.

En los viejos tiempos, para hacer una conexión remota, se marcaba al PBX o servidor terminal para conectarse a un mainframe o minicomputadora como una terminal "tonta". Con el advenimiento de la interconectividad, los servidores de terminal conectados a la red se hicieron cargo de la tarea de responder las llamadas conmutadas. A medida que creció la demanda del cómputo remoto, las conexiones de terminal simple fueron reemplazadas por las que se hacían a través del protocolo SLIP. Para entonces, muchos escritorios contaban con PC en lugar de terminales, pero emulaban terminales para hacer conexiones conmutadas. El auge de la demanda de la conectividad por Internet llevó al mercado a reemplazar SLIP por PPP, un protocolo con aún más capacidad para las comunicaciones de computadora a computadora a través de líneas telefónicas. El PPP presentaba una mejor detección de errores, compresión y soporte para la autentificación. También permitía la conectividad entre varios vínculos (¿alguien desea duplicar su capacidad?). Para nuestros propósitos, supondremos que PPP es el protocolo de marcación telefónica, a menos que se diga otra cosa.

AUTENTIFICACIÓN, AUTORIZACIÓN Y CONTABILIDAD

El marco conceptual de la seguridad basada en el usuario se llama autentificación, autorización y contabilidad (AAA, Authentication, Authorization, Accounting). Este marco conceptual está diseñado para ser consistente y modular, con finalidades fin de proporcionar a los grupos de redes, flexibilidad en la implementación de la directiva de seguridad de la red de la corporación.

NOTA Los sistemas de seguridad de red, como el CiscoSecure Access Control Server (ACS, servidor de control de acceso), controlan el acceso de los segmentos LAN, líneas y aplicaciones de red como HTTP y FTP. Los dispositivos de acceso a la red, generalmente servidores y enrutadores de acceso (controlan el acceso a estos servicios basados en red) pero a veces se configura una capa adicional de seguridad en la plataforma del servidor una vez que se accede a éste. Por ejemplo, un mainframe de IBM hará que se cumplan las directivas de seguridad utilizando sus propios mecanismos. La seguridad para las plataformas de cómputo y los principales paquetes de software todavía se lleva a cabo utilizando sistemas de seguridad que residen en el servidor de aplicación, además de las medidas de seguridad del dispositivo de acceso que se estudian en este capítulo.

Panorama general del modelo AAA

El propósito del AAA es controlar a quién se le permite el acceso a los dispositivos de red y qué servicios pueden utilizar éstos una vez que han accedido. A continuación se presenta una breve descripción de las tres áreas funcionales del modelo AAA:

- **Autentificación** Valida que la identidad del usuario es auténtica antes de otorgar el acceso.
- **Autorización** Otorga al usuario el privilegio de acceder a las redes y los comandos.
- **Contabilidad** Reúne datos para rastrear los patrones de uso por usuario, servicio, host, hora del día, día de la semana, etcétera.

Por fortuna, las personas que diseñaron las siglas pusieron las tres funciones en orden secuencial, haciendo más sencillo recordar el concepto del AAA; primero, se le permite a entrar (se autentifica su identidad); después, tiene ciertos privilegios que puede utilizar una vez que se encuentra dentro (cuenta con autorizaciones predeterminadas) y, por último, se conserva un historial acerca de lo que haga mientras esté dentro del sistema (el grupo de la red mantiene un registro de lo que usted hace).

La filosofía es permitir que los grupos de trabajo impongan las directivas de seguridad en niveles muy específicos. Casi todos los parámetros AAA pueden medirse por segmento LAN, por línea (usuario) y por protocolo (generalmente IP).

AAA es una estructura de implementación de la seguridad definida de manera clara que todos pueden comprender. La arquitectura se define por comando. En realidad, los conceptos del AAA son comandos IOS reales. El inicio de un proceso AAA en un dispositivo Cisco requiere el uso del prefijo **aaa** seguido de una de las tres funciones raíz, como

la de autenticación **aaa authentication**. Por ejemplo, toda una línea de comandos del AAA se podría leer **aaa authentication ppp RemoteWorkers TACACS+ local**. El propósito de AAA es proporcionar la estructura de comandos del lado del cliente sobre la que descansa CiscoSecure.

A continuación se explica cómo habilitar el AAA en un enrutador o servidor de acceso de Cisco.

1. Habilite el AAA utilizando el comando de configuración global **aaa new-model**.
2. Si decide utilizar un servidor de seguridad independiente, configure los parámetros del protocolo de seguridad, como RADIUS, TACACS+ o Kerberos.
3. Defina las listas del método para la autentificación utilizando un comando de autenticación AAA.
4. Aplique las listas del método a una interfaz o línea en particular, si así se requiere.
5. Como opción, puede configurar la autorización utilizando el comando **aaa authorization**.
6. Como opción, puede configurar la contabilidad utilizando el comando **aaa accounting**.

Modularidad AAA

Una directiva de seguridad es un conjunto de principios y reglas adoptadas por una compañía para proteger los recursos de sus sistemas, sus registros confidenciales y la propiedad intelectual. Es responsabilidad del administrador de la red implementar y hacer cumplir la directiva, pero en la realidad, las directivas de seguridad pueden perderse entre la gran cantidad de políticas que se aplican en la oficina, por restricciones de presupuesto y por impaciencia. Un administrador a cargo de usuarios terminales puede tener influencia sobre la manera en que se implantará la directiva en su propio campo. Después de todo, la compañía está financiando la red, no el departamento de tecnología de la información. Por tanto, puede haber mucha variación entre directivas de seguridad (aun dentro de la interconexión de la compañía).

Lo anterior significa que las directivas de seguridad deben ser muy adaptables. El CiscoSecure ACS trata de satisfacer esta necesidad con la modularidad (es decir, la capacidad de aplicar por separado las funciones de seguridad por entidad asegurada, independientemente de la manera en que éstas se apliquen a otros recursos). La arquitectura del AAA le proporciona la opción de implementar cualquiera de las tres funciones de manera independiente a las otras dos. Esto incluye si dichas funciones están activadas en un dispositivo, cuál protocolo de seguridad utilizan y a qué servidor de seguridad o base de datos de usuario se acceda.

Controles de autentificación El comando **aaa authentication** valida una identidad de usuario en el momento de ingresar. Pero una vez que ha sido autentificado, ¿exactamente a qué puede acceder? Esto depende del tipo de acceso que se aplique:

- Si es un administrador de red que accede a un conmutador para hacer un pequeño ajuste en su archivo config, la autentificación lo conduce a la solicitud del comando IOS del conmutador.
- Si es un empleado que está dentro de la empresa y lo autentificó un enrutador, accedería a un host protegido para operar Windows o las aplicaciones cliente-servidor de interconexiones basadas en el navegador.

- Si trabaja en casa y lo autentifica un servidor de acceso, sería admitido a la interconexión de su empresa para operar las mismas aplicaciones cliente-servidor.
- ▲ Si marcó a Internet desde casa, como miembro del público en general, habría sido autentificado por uno de los muchos servidores de acceso de su ISP, y habría entrado a Web.

La autentificación debe encargarse de proteger tres entornos de destino: Internet, la interconexión y, ante todo, el sistema operativo interno de los dispositivos en que funcionan las interconexiones. En la figura 6-3 se ilustran los tipos de acceso y los entornos de destino.

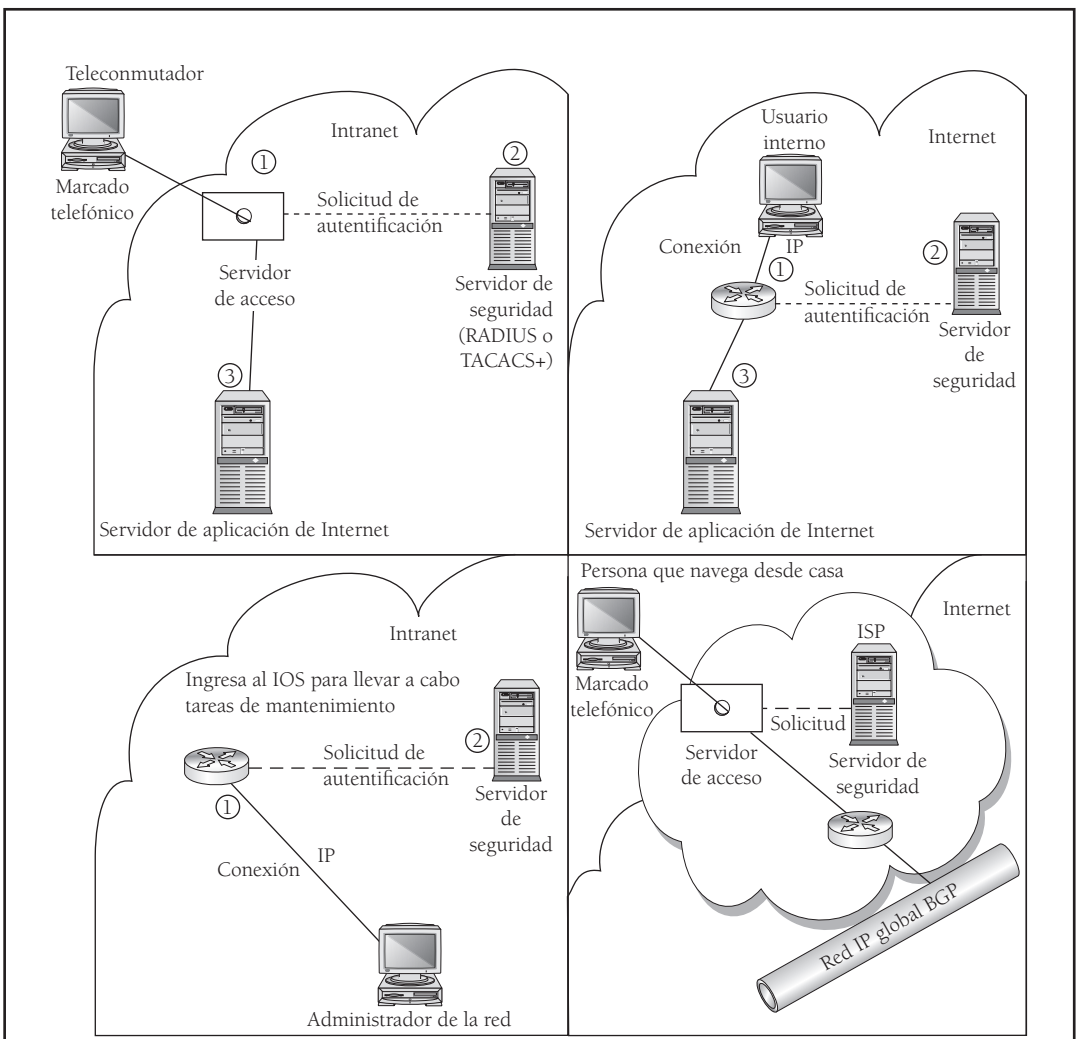


Figura 6-3. La autentificación se lleva a cabo en cuatro escenarios que brindan acceso a tres mundos.

El escenario en que el administrador de la red accede a los dispositivos IOS es único. En las interconexiones de Cisco, ese tipo de acceso suele autentificarse mediante el uso de TACACS. Los administradores de las redes acceden a un entorno IOS del dispositivo para realizar tareas relacionadas con la administración del dispositivo.

Los usuarios también requieren diferentes servicios de marcación telefónica. A pesar de que la mayoría utiliza PPP en estos días, aún se pueden presentar diferentes necesidades. En función de la red local desde la que se realice la llamada, tal vez se requieran diferentes servicios PPP, como IP, IPX, NetBEUI o sólo una conexión terminal.

Cualesquiera que sean los problemas, a menudo los diferentes requisitos llevan al uso de varios métodos de autentificación en la misma interconexión. CiscoSecure ACS le permite al administrador de la red el uso de cualquiera de los principales protocolos de marcado y las técnicas de autentificación. Además, éste soporta la capacidad de aplicar estas diferentes herramientas en la interfaz de red o en línea (aun en el mismo dispositivo).

Controles de autorización La autorización AAA limita los servicios al usuario. En otras palabras, si se ha activado la autorización en una entidad segura utilizando el comando **aaa authorization**, los usuarios deben tener explícitamente el acceso a dicha entidad.

El perfil de usuario de la persona suele almacenarse en el servidor de seguridad y a veces también en la base de datos del usuario local del dispositivo. Cuando el administrador

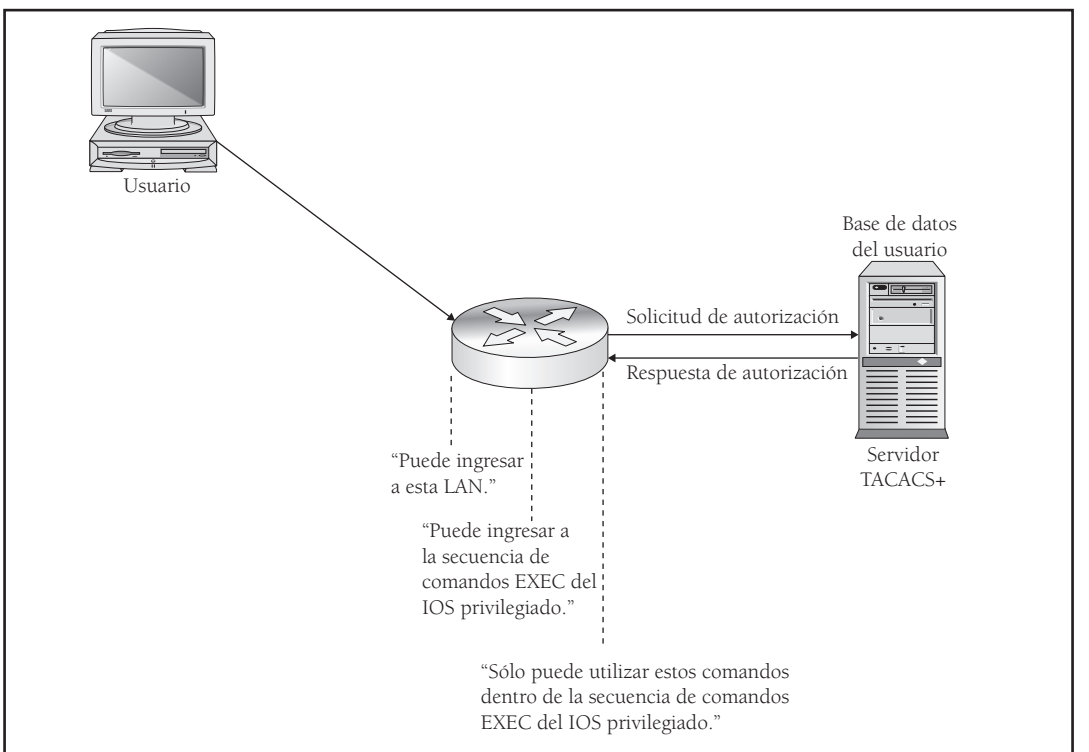


Figura 6-4. Las autorizaciones pueden imponerse por la red, el modo de comando y aun por el comando.

se registra en el dispositivo y se verifica su perfil de usuario, el dispositivo configura las autorizaciones para saber cuáles comandos se permite usar al administrador durante esa sesión. Los comandos pueden autorizarse por el modo de comandos del IOS (los indicadores de comandos MyRouter: en comparación con MyRouter#) o por comandos específicos dentro de un modo. En la figura 6-4 se describen algunas de las diferentes formas que pueden tomar las autorizaciones.

Las autorizaciones pueden ser más complicadas que las autentificaciones. Después de que ha sido autentificado, el servidor de seguridad debe proporcionar la información acerca de la configuración del dispositivo de acceso específica del usuario (por ejemplo, a qué redes puede acceder el usuario, qué tráfico de aplicación puede operar, qué comandos está bien utilizar, etcétera). Sin el mantenimiento centralizado de la información de autorización, no sería práctico asignar autorizaciones por usuario. (Es muy difícil mantener actualizados los nombres y contraseñas de los usuarios.)

Controles de contabilidad La contabilidad no permite o niega nada, en cambio conserva un registro activo de qué hacen los usuarios. La contabilidad del AAA es un proceso tras bambalinas que rastrea los accesos de las personas y el uso de la red. En la figura 6-5 se muestra cómo la contabilidad de seguridad del AAA rastrea el uso de los recursos.

La contabilidad del AAA refleja eventos conforme se presentan al entrar a los sistemas y utilizar los servicios. Por tanto, los comandos de contabilidad son, más o menos, reflejos de los demás. Por ejemplo, las tareas de contabilidad pueden habilitarse por sistema, por el modo comando, por la interfaz de dispositivo de red, por protocolo y por conexión (de la misma forma que los comandos de autorización).

NOTA Como opción predeterminada, el AAA define el IOS como un sistema que cuenta con dos modos de comando: el modo EXEC de usuario (a veces llamado secuencia de comandos o Shell) y los modos EXEC privilegiados. El comando **nivel** del IOS se utiliza para dividir cosas en 16 niveles de comando (numerados del 0 al 15), de modo que el acceso a los comandos puede autorizarse de manera más específica.

Tendencias que llevan a sistemas de seguridad cliente-servidor

Al igual que con casi todos los sistemas de control de red, el AAA utiliza el modelo cliente-servidor para administrar la seguridad. En otras palabras, hay un servidor central de seguridad que almacena la información relacionada con el perfil del usuario que utilizan los dispositivos de acceso al cliente para imponer la seguridad. Cuando un usuario hace una solicitud para conectarse a una red, línea o servicio, el dispositivo del cliente solicita al servidor que verifique si está bien. La centralización es necesaria, porque no es factible administrar la seguridad de dispositivo de acceso en dispositivo; simplemente existen demasiados como para tener un registro de los mismos.

En la década de 1970, un producto natural de los usuarios remotos que marcaban a los mainframes centrales era que los perfiles de seguridad del usuario (cuentas, contraseñas y autorizaciones) estaban almacenados justamente en la misma computadora donde residían todos los servicios. Esto hizo que los sistemas de seguridad verificaran de manera sencilla los permisos de los usuarios. Después, en la década de 1980, las minicomputadoras depar-

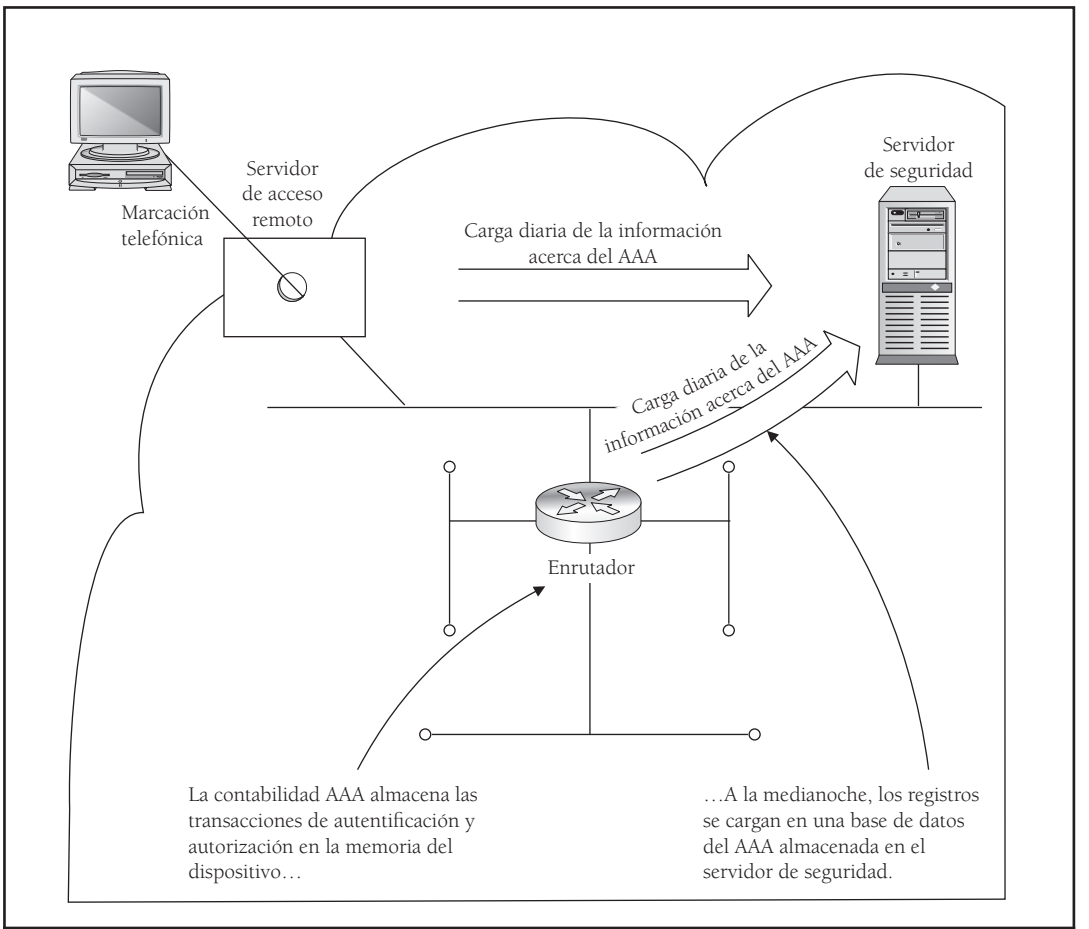


Figura 6-5. La contabilidad del AAA es un proceso tras bambalinas que registra la actividad de red de un usuario.

tamentales se hicieron populares, extendiéndose por toda la empresa. Se inventaron los servidores de terminal para proporcionar los puntos de acceso adicionales que requerían las topologías distribuidas, pero las bases de datos de los usuarios estaban ahora distribuidas en muchos dispositivos de acceso (dificultando más el mantenimiento de los sistemas de seguridad). Cuando surgió la conectividad basada en IP, se hizo evidente que la información de seguridad tenía que estar centralizada. En la figura 6-6 se muestra esta tendencia.

El surgimiento de la interconectividad demanda que una empresa ofrezca acceso por marcado telefónico en toda la organización. Esto presenta problemas para imponer controles consistentes de seguridad en muchos servidores de acceso. La arquitectura AAA es el plan de ataque de Cisco para enfrentar estos retos. Además, los servidores TACACS+ y RADIUS pueden integrarse con servicios como Active Directory de Microsoft, permitiendo la centralización de la información del AAA.

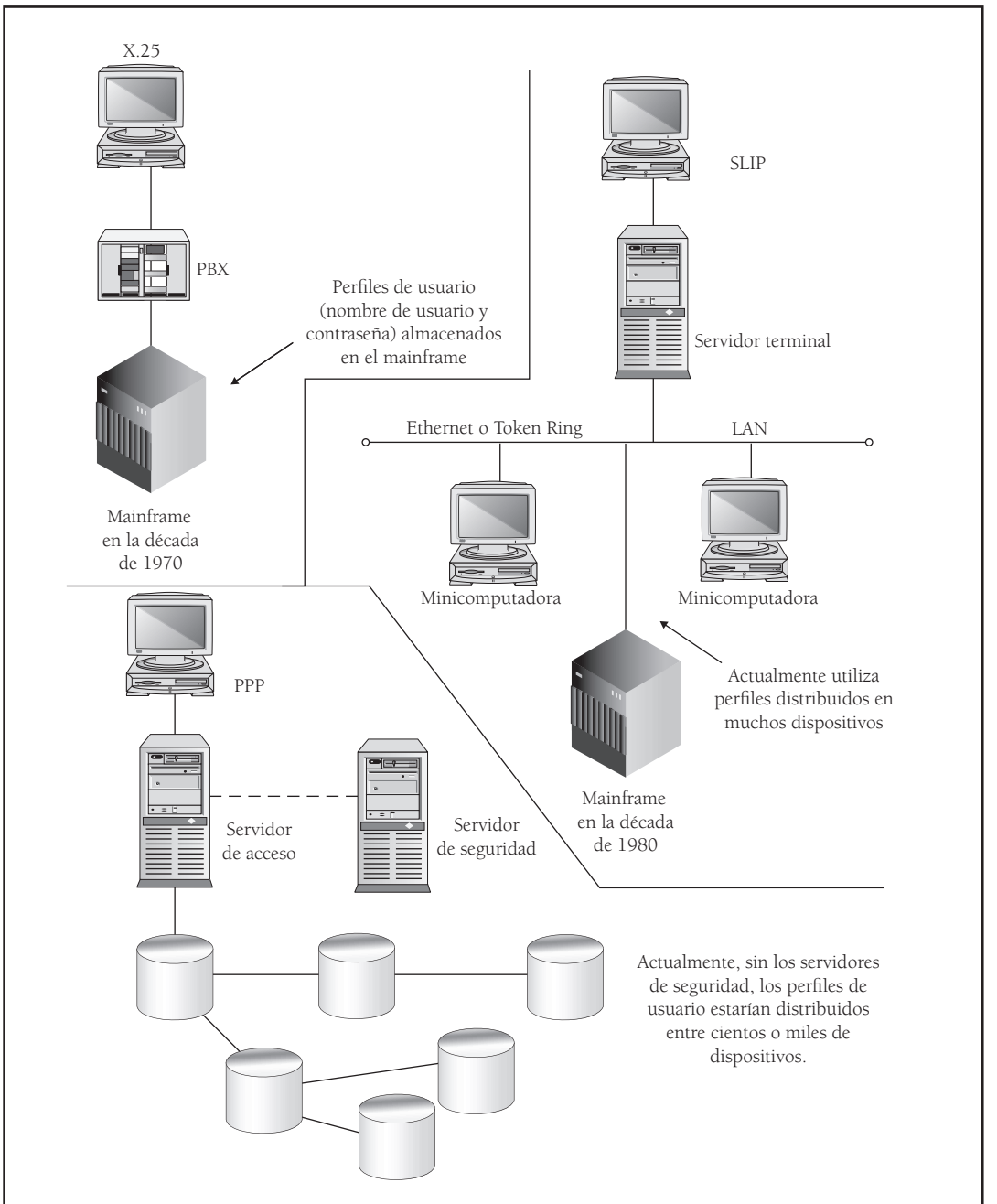


Figura 6-6. Los sistemas de seguridad han evolucionado paralelamente a la industria de la computación.

Dos protocolos de seguridad del AAA: TACACS+ y RADIUS

Es posible utilizar la seguridad del AAA en forma independiente, sin una base de datos central de seguridad. En la realidad, sólo algunos hacen esto porque se requeriría un esfuerzo adicional para mantener los parámetros de seguridad dispositivo por dispositivo (una propuesta susceptible al error y muy laboriosa). El IOS soporta la seguridad independiente porque, en algunos casos, no se encuentra disponible un servidor de seguridad (por ejemplo, en una interconexión muy pequeña o durante el periodo en que se está implementando un servidor de seguridad y, por ende, no está trabajando).

AAA configura los dispositivos de acceso como clientes. Entre los dispositivos cliente se incluyen los servidores de acceso, los enrutadores, los conmutadores y los firewalls. Los clientes solicitan que uno o más servidores de seguridad verifiquen si están permitidas las conexiones de usuario. Para lo anterior, es necesario contar con un protocolo para especificar las reglas y convenciones que rigen el intercambio de información. La seguridad del AAA puede utilizar dos protocolos para manejar las configuraciones de seguridad cliente-servidor:

- **RADIUS** Es un protocolo de seguridad utilizado principalmente para autentificación. RADIUS son las siglas de Remote Authentication Dial-in User Service (servicio de autentificación remota para usuarios de marcación telefónica). RADIUS es un estándar de la industria bajo los auspicios del IETF (Internet Engineering Task Force).
- **TACACS+** Es un protocolo propiedad de Cisco que, en gran medida, es equivalente a RADIUS, pero con una mayor integración de la autorización y la contabilidad con la autentificación. TACACS son las siglas de Terminal Access Controller Access Control System (sistema de control de acceso al controlador de acceso a terminal). Cisco ha puesto a consideración del IETF, el TACACS+ como un protocolo estándar de seguridad.

NOTA Existe un tercer protocolo de seguridad llamado Kerberos, que fue desarrollado en el MIT y es un estándar abierto para la autentificación de claves secretas que utiliza el algoritmo criptográfico Data Encryption Standard (DES, estándar de cifrado de datos). Hace algunos años, Microsoft, por ejemplo, integró a Kerberos en Windows 2000. Aunque es más difícil de implementar y administrar, Kerberos está ganando popularidad en las interconexiones más sensibles a la seguridad: sus beneficios principales son que puede funcionar en una red con equipo de fabricantes múltiples como RADIUS, pero no transmite contraseñas por la red (en cambio, pasa los llamados tickets). El IOS incluye comandos de Kerberos en su estructura de AAA.

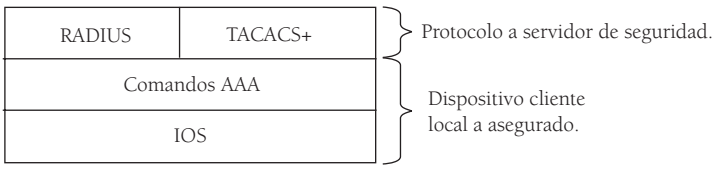
Cómo trabaja el AAA

AAA es la infraestructura de seguridad de los dispositivos IOS. Los comandos AAA residen en el modo EXEC privilegiado del IOS. Cada dispositivo cliente está configurado para la seguridad utilizando los comandos AAA del modo de configuración global. Si se configura adecuadamente, el dispositivo puede usar el servidor CiscoSecure utilizando los protocolos de seguridad TACACS+ o RADIUS, o ambos.

En realidad, los comandos del AAA pueden utilizarse en forma independiente para asegurar los dispositivos. En otras palabras, el dispositivo puede utilizar una base de da-

tos local de usuario almacenada en NVRAM en el dispositivo en sí, en lugar de uno en un servidor RADIUS o TACACS+. Sin embargo, esto se hace muy rara vez, porque implica el mantenimiento y el monitoreo de los datos de seguridad del usuario en cientos o miles de archivos config de dispositivo en lugar de una sola base de datos.

TACACS+ y RADIUS son protocolos de red cliente-servidor que se utilizan para implantar la seguridad cliente-servidor en la red. En ese sentido, son el equivalente de lo que es el SNMP a la administración de la red.



Una base de datos del usuario cambia cada vez que se agregan o eliminan usuarios, se cambian las contraseñas o se modifican las autorizaciones. La separación de la base de datos del usuario de los archivos config del dispositivo reduce el número de lugares en que se deben realizar actualizaciones. Casi todas las interconexiones utilizan un servidor principal y uno o dos servidores de seguridad alternos, dejando sólo algunos lugares en que las bases de datos del perfil del usuario necesitan actualizarse.

La *sincronización de la base de datos* consiste en asegurarnos que las bases de datos de los usuarios contienen datos idénticos. Esto puede hacerse automáticamente configurando Replication Partners en CiscoSecure ACS. En un escenario con tres servidores de seguridad, las tres bases de datos de usuario se podrían configurar como socios de réplica y CiscoSecure ACS sincronizaría automáticamente los registros de los perfiles de usuario entre las tres todos los días.

Además de los archivos de usuario, el servidor puede sincronizar cualquiera de los siguientes elementos:

- ▼ La base de datos de usuarios y grupos.
- ■ La base de datos del grupo solamente.
- ■ Las tablas del dispositivo para la configuración de la red.
- ■ La tabla de distribución.
- ■ La configuración de la interfaz.
- ■ Los parámetros de seguridad de la interfaz.
- ■ Los parámetros de validación de las contraseñas.
- ■ Directivas y llaves maestras del EAP-FAST.
- ▲ Directivas del CNAC.

El proceso de aprobación del AAA

El AAA funciona compilando atributos que especifican los permisos de un usuario. En el contexto del AAA, un *atributo* es un apuntador hacia la entidad (u objeto) al que la persona puede tener acceso. Por ejemplo, un atributo de autentificación podría ser un segmento LAN específico al que se le permite el acceso a la persona. Un atributo de la autorización podría ser el límite de conexiones concurrentes que la persona pudiera tener abiertas en determinado momento.

Cuando un usuario intenta conectarse a un servicio seguro, el dispositivo de acceso verifica si el usuario cuenta con la autorización de la directiva de seguridad. Esto lo hace enviando una solicitud a la base de datos del servidor para verificar si hay un nombre que coincida. El dispositivo de acceso seguro sabe qué solicitar con base en sus valores de los parámetros del archivo config, y se utiliza la consulta para verificar que el usuario tiene permiso para hacer cualquier cosa que se trate de hacer.

Pares atributo-valor La solicitud contiene los atributos que son obligatorios para el servicio solicitado, como se define en el archivo config del dispositivo de acceso. El servidor procesa la solicitud buscando los mismos atributos en el perfil del usuario en la base de datos del usuario. Esta búsqueda es para encontrar los atributos-valores. Un atributo, llamado *par atributo-valor* (o par AV) en la terminología de TACACS+, es un término gracioso para describir la representación de una entidad de red que es segura.

Por ejemplo, en el perfil de usuario de alguien, la contraseña es un atributo y la contraseña real de la persona, *realmentesoyyo*, es el valor asociado con ésta. Cuando el usuario ingresa la contraseña, el dispositivo de acceso que maneja el inicio de sesión sabe que primero hay que verificar una contraseña, porque el hacer esto está establecido como un parámetro en el archivo config del dispositivo. Al verificar el perfil del usuario de la persona, busca una coincidencia ente el valor ingresado en la solicitud de contraseña y lo que está en el archivo de la base de datos del usuario como el nombre de usuario que ingresó la persona. En la figura 6-7 se muestra el procedimiento AAA para el manejo de una solicitud de conexión por parte del usuario.

Cómo maneja AAA las transacciones de autentificación Cuando se establece una conexión, el dispositivo de acceso contacta al servidor de seguridad y despliega una solicitud de usuario. El usuario ingresa la información (por lo general, solamente un nombre de usuario y una contraseña), y el protocolo (RADIUS o TACACS+) codifica el paquete y lo manda al servidor. El servidor decodifica la información, verifica el perfil del usuario, forma y codifica la respuesta y regresa ésta al dispositivo de acceso.

Las reglas de aprobación del AAA son muy sencillas: si se regresa un ACCEPT, se lleva a cabo la conexión solicitada. Si se regresa un REJECT, la sesión de solicitud de conexión del usuario se termina. Pero si regresa un ERROR y el dispositivo de acceso está configurado para varios servidores de seguridad, la solicitud es entonces enviada hacia un servidor alterno. Si ese servidor tampoco regresa una respuesta, el proceso continúa hasta que se le acaban los servidores a la solicitud. En este punto, si el dispositivo de acceso se ha configurado por un segundo método, de nuevo iterará a través del proceso, buscando primero la aprobación con la solicitud al servidor principal de seguridad, etcétera. Si el dispositivo de acceso se satura con métodos de autentificación, éste termina la sesión de solicitud de conexión del usuario.

La respuesta CONTINUE es otro parámetro opcional de configuración que solicita información adicional al usuario. Las solicitudes pueden ser cualquier cosa que el administrador de red defina arbitrariamente. Por ejemplo, un reto común es solicitar a los usuarios su apellido.

NOTA Un daemon (demonio) es un proceso que opera en un servidor para llevar a cabo una tarea predefinida, por lo general como respuesta a algún evento. El término viene de la mitología griega, en que los demonios eran espíritus guardianes. A los daemons se les

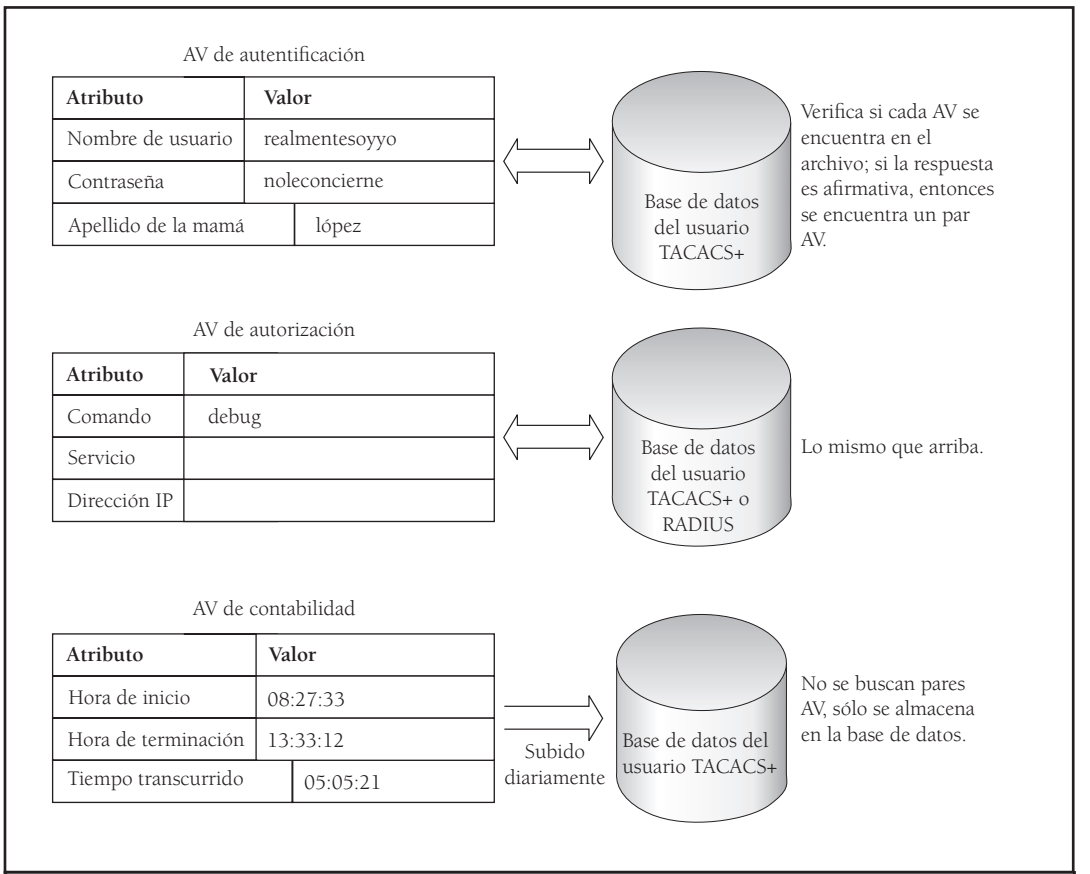


Figura 6-7. Las solicitudes de acceso de los usuarios se otorgan si los valores-atributo coinciden en el perfil del usuario.

denomina agentes del sistema en terminología de Windows. Un daemon del TACACS+ reside en el servidor de seguridad y llena solicitudes de autentificación o autorización desde los dispositivos de acceso de los clientes. Lleva a cabo lo anterior al buscar, en la base de datos del usuario, los pares AV requeridos y regresando los resultados al cliente en la forma de paquetes TACACS+.

Transacciones de autorización Si el usuario se autentifica, se contacta el daemon para verificar los atributos de autorización caso por caso. En la figura 6-8 se muestra cómo la autentificación y la autorización trabajan juntas.

Pueden generarse atributos de autorización para servicios como tipo de conexión (inicio de sesión, PPP, etcétera), modos de comandos del IOS (EXEC de usuario y EXEC privilegiado) y varios parámetros de conexiones, incluidas las direcciones IP de host, las interrupciones del usuario, las listas de acceso, etcétera. Por naturaleza, la autorización es más sofisticada que la autentificación. Se encuentra implícita más información que sólo el nombre y la

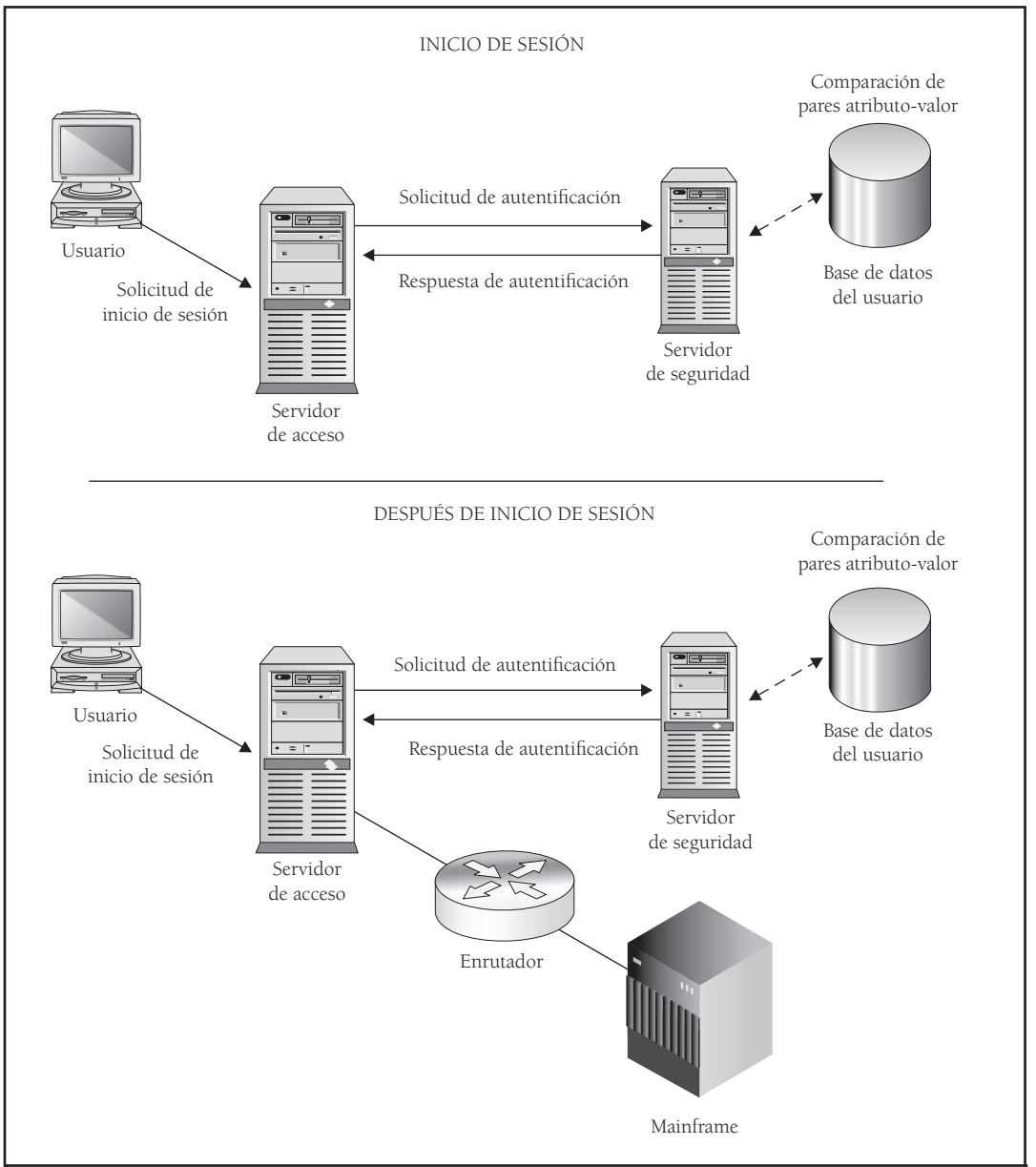


Figura 6-8. Una vez autentificado, las autorizaciones de un usuario se borran a medida que se requieran.

contraseña del usuario y los atributos tienen un estado. Por ejemplo, el atributo Maximum-Time (tiempo máximo) requiere que el servidor mantenga registros sobre cuánto tiempo ha estado conectado el usuario y que termine la sesión cuando se ha excedido el valor para el usuario (número de segundos).

Protocolos de autentificación

CiscoSecure ACS soporta varios mecanismos de autentificación. También se llaman *configuraciones de contraseña* o *protocolos de contraseña* y son protocolos de autentificación que se aseguran de que usted sea quien dice ser cuando ingresa al sistema. Aquí se encuentran cuatro mecanismos principales de autentificación que soporta el AAA:

- ▼ **ASCII** El American Standard Code for Information Interchange (código estándar estadounidense para el intercambio de información) es el protocolo de autentificación más antiguo. ASCII es una técnica que depende de la máquina para representar caracteres en inglés, y tiene muchos otros usos además de la autentificación. La autentificación con ASCII requiere que el usuario teclee un nombre de usuario y una contraseña para enviarla en texto simple (es decir, sin cifrado) y que se compare con los que se encuentran en la base de datos del usuario almacenados en formato ASCII.
- ■ **PAP** El Password Authentication Protocol (protocolo de autentificación de contraseñas) se utiliza para autentificar las conexiones PPP. El PAP pasa las contraseñas y otra información del usuario en formato de texto. Se conoce al PAP como un protocolo que le permite almacenar su nombre de usuario y contraseña en el cuadro de diálogo, de tal forma que no tenga que teclearlo cada vez que ingrese al sistema.
- ■ **CHAP** El Challenge Handshake Authentication Protocol (protocolo de desafío de autentificación de saludo) proporciona la misma funcionalidad que el PAP, pero es mucho más seguro, porque elimina el envío de la contraseña y demás información del usuario a través de la red hacia el servidor de seguridad. En la figura 6-9 se muestra cómo funciona el desafío de respuesta.
- ▲ **Token-Card** Esta técnica de autentificación utiliza contraseñas de una sola vez. Una tarjeta token es un dispositivo electrónico un poco mayor que una tarjeta de crédito. Se utiliza para generar una contraseña cifrada que debe coincidir con una llenada para el usuario en la base de datos de tarjetas token que reside en el servidor de seguridad. La contraseña cifrada sólo es válida para una sola vez; de ahí el nombre *token*. Los sistemas de autentificación de token-card proporcionan la mejor seguridad de acceso.

AAA también soporta NASI (NetWare Asynchronus Services Interface, interfaz para los servicios asincrónicos de NetWare), que es un protocolo de autentificación incluido en las LAN de Novell. Otro protocolo de contraseña específico de un fabricante es el ARAP (AppleTalk Remote Access Protocol), con un doble mecanismo de autentificación de desafío de respuesta que lleva al CHAP un paso más adelante haciendo que el servidor de seguridad también se autentifique *así mismo* ante el cliente. Además, existen pequeñas variaciones en cuanto a la forma en que el protocolo PAP trabaja con Windows NT/2000/2003.

La seguridad tiene un precio (sobre todo en la forma de una creciente inconveniencia para los usuarios), pero por otro lado también tiene la ventaja de implantar y administrar medidas de seguridad. Por ejemplo, CHAP requiere hardware y experiencia adicionales y el uso de las tarjetas token es muy problemático. ¿Se imagina a un enorme proveedor de servicios de Internet, como AOL, enviando por correo tarjetas token a cada nuevo usuario y administrando una base de datos de token de contraseñas de una sola vez? El gasto adicional y la complejidad logística de los protocolos de autentificación avanzados han evitado su adopción.

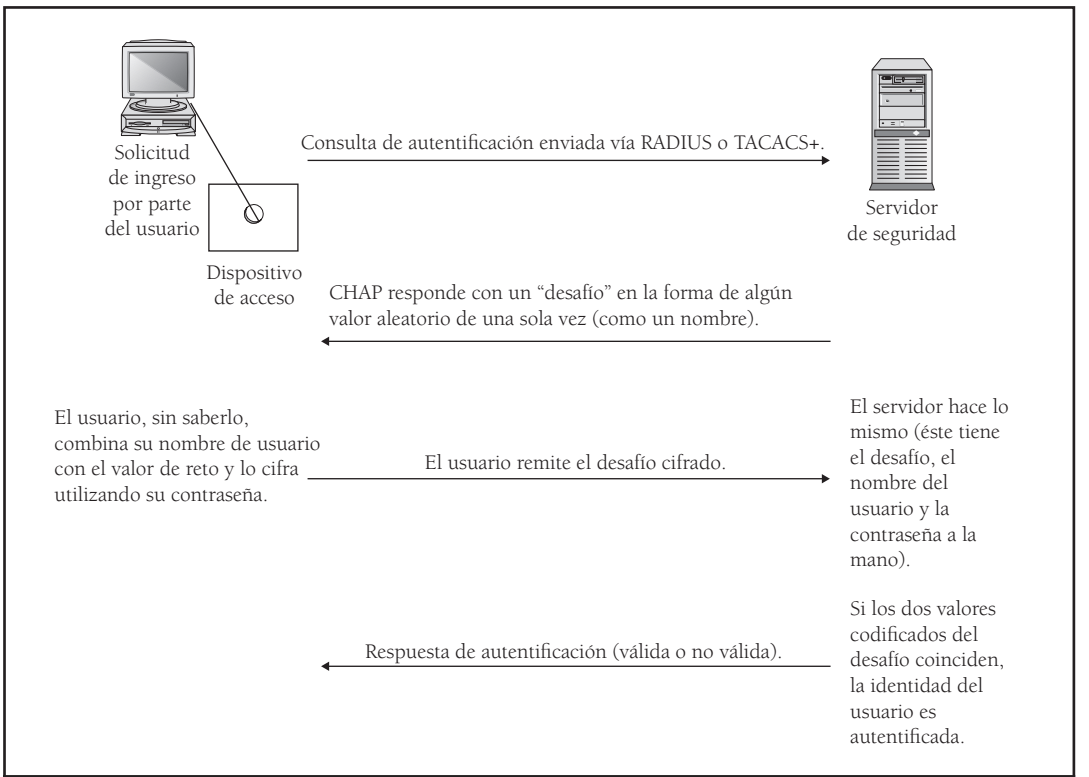


Figura 6-9. La autentificación de CHAP no envía la contraseña por la red.

Existen ciertas razones por las que PAP ya no es el favorito sobre EAP, CHAP y MS-CHAP. Las interconexiones corporativas suelen utilizar CHAP, mientras que las tarjetas token se utilizan principalmente para proteger a las redes de alta seguridad en la milicia, los centros de investigación y desarrollo, los bancos y otros ambientes sensibles a la seguridad.

Métodos y tipos

Ciertas partes deben ponerse en su lugar antes de imponer la seguridad. Como acaba de ver, el dispositivo de acceso debe configurarse para solicitar uno o más servidores de seguridad para la autentificación y la autorización, y la base de datos del usuario debe tener los perfiles que contengan los atributos que definan qué se le permite hacer al usuario en la red. Pero, ¿qué pasa exactamente cuando una solicitud coincide con la base de datos TACACS+ o RADIUS? ¿Qué pasos se toman para verificar la identidad del usuario y establecer qué servicios se le pueden permitir a esa persona?

Las premisas de los comandos de AAA en el archivo config de un dispositivo de acceso le indican al dispositivo qué hacer cuando un usuario trata de ingresar. Los comandos raíz del AAA, **authentication**, **authorization** y **accounting**, se utilizan en conjunto con varias claves para codificar las instrucciones del archivo config acerca de cómo se van a manejar los intentos de conexión. Como ya se mencionó, los parámetros de esta instrucción son mo-

dulares en el sentido de que pueden aplicarse por usuario y por servicio. Las instrucciones se implementan en el archivo config del dispositivo de acceso utilizando métodos y tipos:

- ▼ Un *método* es un programa de cómputo preempacado que lleva a cabo una función específica. Por ejemplo, **radius** es un método para solicitar un servidor RADIUS.
- ▲ Un *tipo* es una entidad en que se aplica el método. Por ejemplo, el método **radius** se aplica a un tipo **ppp** de tal forma que cuando un usuario intente hacer una conexión utilizando el protocolo PPP, el dispositivo de acceso consulta su servidor RADIUS para autentificar la identidad de la persona.

Debido a que casi siempre existen varios parámetros de seguridad configurados para un dispositivo, a las configuraciones del AAA se les conoce como *listas de métodos con nombre*, porque el administrador les asigna un *nombre* en el archivo config del dispositivo y se aplican a uno o más tipos específicos de entidad asegurada. En la figura 6-10 se muestra cómo las listas y los tipos del método con nombre trabajan en conjunto para imponer la seguridad.

NOTA Existen métodos sin nombre en la forma de la lista de métodos predeterminados. Si una interfaz o línea no tiene lista de métodos con nombre configurada, automáticamente se le asigna en forma predeterminada una lista de métodos. Para no contar con seguridad AAA, se debe configurar explícitamente de esta forma mediante el uso del método **none**. El comando se vería así: **aaa accounting none**. Cisco dificulta las opciones de no tener seguridad.

Las listas de métodos con nombre se ingresan en el archivo config del dispositivo de acceso que se está asegurando (por lo general, un servidor de acceso o un enrutador). El IOS

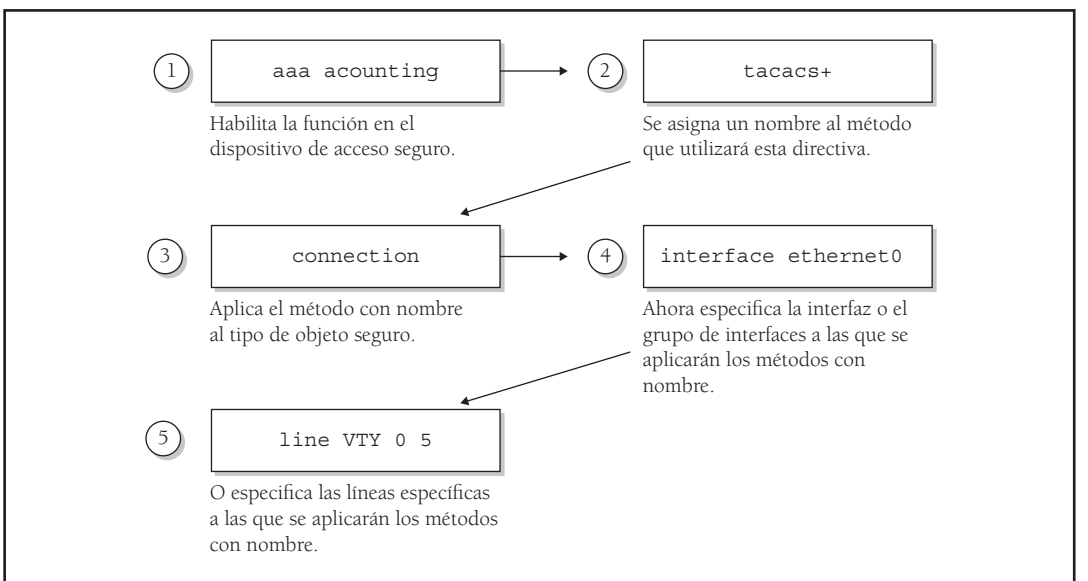


Figura 6-10. Las listas de métodos con nombre hacen que se cumplan las directivas de seguridad en las interfaces de los dispositivos de acceso.

Utilice la base de datos de copia de seguridad de los usuarios en el dispositivo mismo, si el servidor no responde.

Éstos son tipos de AAA.

Habilita AAA en el dispositivo.

```
MyRouter(config)#aaa new-model
```

Determina cuatro listas de métodos (sombreados) usados para asegurar el dispositivo.

```
MyRouter(config)#aaa authentication login NetworkTeam local
MyRouter(config)#aaa authentication ppp RemoteWorkers radius local
MyRouter(config)#aaa authorization network NoWay tacacs+ local
MyRouter(config)#aaa accounting network KeepWatch start-stop tacacs
```

```
username root password HushHushHush
```

Asigna un nombre a los servidores de seguridad que se utilizarán.

Establece la seguridad cliente-servidor.

```
MyRouter(config)#radius-server host VelteAccess
MyRouter(config)#tacacs-server host VelteManager
MyRouter(config)#radius-server key GobbledyGook
MyRouter(config)#tacacs-server key GobbledyGook
```

Proporciona al dispositivo la clave de acceso compartido para ingresar a los servidores.

Aplica seguridad a objetos específicos, aquí PPP se conecta a más de un grupo de 16 interfaces.

```
MyRouter(config)#interface group-async NumeroUno
MyRouter(config-if)#group-range 1 16
MyRouter(config-if)#encapsulation ppp
MyRouter(config-if)#ppp authentication chap RemoteWorkers
```

Indica al servidor de acceso que comience una conexión PPP cuando éste conteste el teléfono.

```
MyRouter>(config)#line 1 16
MyRouter>(config)#autoselect ppp
MyRouter>(config)#autoselect during-login
MyRouter>(config)#login authentication NetworkTeam
MyRouter>(config)#modem dialin
```

Figura 6-11. Las partes básicas de un modelo de configuración de seguridad tienen gran cantidad de parámetros.

aplica los métodos en la secuencia en que éstos aparecen en la configuración, tratando desde el principio el primer método y luego trabajando con los siguientes hasta que se recibe un ACCEPT o REJECT. En la figura 6-11 se explica una lista de métodos con nombre típica.

La última parte de la configuración de AAA de la figura 6-11 especifica líneas, porque la autentificación tiene que ver con los usuarios individuales. La seguridad basada en el tráfico puede aplicarse en la interfaz, porque el firewall o enrutador supervisa la información en el encabezado de cada paquete (un proceso que se lleva a cabo ya sea sobre todos o ninguno de los paquetes que pasan por una interfaz). En contraste, la seguridad basada en el usuario controla a las personas a medida que éstas realizan una conexión a una red remota mediante un servidor de acceso o ingresan al IOS dentro de un enrutador o conmutador de la red. Cada uno de estos escenarios requiere el uso de una línea.

Métodos y tipos de autentificación de AAA AAA cuenta con varios métodos para autentificar la identidad de un usuario. Sólo se puede utilizar un método por línea de usuario (excepto cuando el método **Local** está configurado como respaldo de uno de los tres métodos cliente-servidor). En la tabla 6-1 se ofrece una lista con los métodos de autentificación de Cisco.

La lista de los métodos del AAA de la tabla 6-1 varía ligeramente en función del mecanismo de contraseña que se esté utilizando. Recuerde que AAA es un modelo arquitectónico que debe ser adaptado a las diferencias en la forma en que otros fabricantes diseñan sus productos. Por ejemplo, AAA soporta los métodos Guest y Auth-Guest para el protocolo de contraseñas del ARAP de Apple.

Palabra clave del comando del IOS	Método de autentificación AAA
Group RADIUS	Autentifica mediante el protocolo RADIUS y la base de datos del usuario.
Group TACACS+	Autentica mediante el protocolo TACACS+ y la base de datos del usuario.
Group *nombre de grupo*	Autentifica mediante un subconjunto de servidores RADIUS y TACACS+ para la autentificación como la definen los comandos **aaa group server radius** y **aaa group server tacacs+**.
Krb5	Autentifica mediante el protocolo Kerberos 5 y la base de datos del usuario. (Nota: Kerberos sólo puede utilizarse con el protocolo de contraseñas del PAP.)
Krb5-telnet	Utiliza el protocolo de autentificación Kerberos 5 telnet cuando la conexión utiliza Telnet.
Local	Autentifica mediante una base de datos del usuario almacenada en memoria en el dispositivo de acceso, o para respaldo, si el servidor de seguridad no responde.
Line	Autentifica mediante la contraseña Line para autentificación.
Local-case	Autentifica mediante la autentificación de nombre de usuario local sensible a mayúsculas y minúsculas.
Cache *nombre del grupo*	Autentifica mediante un grupo de la memoria caché del servidor.
Enable	Autentifica mediante las contraseñas Enable Secret en el archivo config del dispositivo de acceso.
None	No utiliza autentificación.

Tabla 6-1. Métodos de autentificación del IOS.

Es posible configurar diferentes métodos de autentificación en distintas líneas dentro del mismo dispositivo de acceso. Por ejemplo, es posible que quiera configurar conexiones PPP para consultar la base de datos del usuario en un servidor RADIUS, pero verificar la base de datos local del usuario para las conexiones de acceso hechas desde el puerto AUX o el puerto de la consola.

Tipos de conexiones Debido a que la autentificación se aplica a las líneas de usuario, los métodos de autentificación con nombre se aplican a los tipos de conexiones. Un *tipo de conexión* es el protocolo de comunicaciones que se utiliza para establecer una conexión. La explicación es que, en la actualidad, las conexiones remotas hacia los ISP y las interconexiones suelen ser conexiones PPP. Pero cuando un administrador de red ingresa al IOS para trabajar en un dispositivo, esa conexión se lleva a cabo a través de una sesión Telnet (si se hace por la red) o de un emulador de terminal (si se hace por medio de los puertos AUX y de consola). En la tabla 6-2 se explican los tipos de autentificación.

El ejemplo de instrucciones siguiente ilustra una interfaz serial en un servidor de acceso que está siendo configurado para utilizar TACACS+ para autentificar a las personas que realizan conexiones con mediante el protocolo PPP.

```
MyAccessServer(config)#aaa new-model
MyAccessServer(config)#aaa authentication ppp MyList tacacs+ local
MyAccessServer(config)#interface serial0
MyAccessServer(config-if)#ppp authentication pap MyList
MyAccessServer(config)#tacacs-server host 10.1.13.10
MyAccessServer(config)#tacacs-server key DoNotTell
```

El comando **aaa new-model** activa (habilita) AAA dentro del software del IOS del dispositivo. Luego, la instrucción especifica que se utilice un protocolo de seguridad TACACS+

Palabra clave del comando del IOS	Tipo de autentificación de AAA
Login	Conexiones de línea con interfaces de red de Ethernet y Token Ring mediante Telnet o hacia los puertos AUX y de la consola mediante terminal virtual (VTY).
PPP	Conexiones de línea de marcado telefónico con interfaces de red seriales mediante el protocolo punto a punto.
SLIP	Conexiones de línea de marcado telefónico con interfaces de red seriales mediante el protocolo de Internet de línea serial.
ARAP	Conexiones de línea de marcado telefónico con interfaces de red seriales utilizando el protocolo de acceso remoto de AppleTalk.

Tabla 6-2. Tipos de entidad asegurada por los métodos de autentificación de AAA.

y que la base de datos local del usuario debe utilizarse si el servidor TACACS+ no llega a responder. El comando **interface serial10** indica la configuración a todas las líneas en la interfaz de red serial del servidor de acceso que estuvieran nombradas como serial10. El comando **ppp authentication pap MyList TACACS+ local** especifica que el protocolo de contraseña del PAP se utilice para conexiones PPP y que se aplique la lista del método con nombre **MyList** para utilizarse como la prueba.

La instrucción siguiente especifica que el servidor del TACACS+ reside en la computadora anfitriona en la dirección IP 10.1.13.10. La línea siguiente especifica que se utilice la clave de decodificación **DoNotTell** para todas las comunicaciones entre el servidor de seguridad y el dispositivo de acceso al cliente que se está configurando aquí. La clave de codificación compartida también debe configurase en el o los servidores de seguridad con que se comunicará el dispositivo de acceso al cliente.

NOTA En AAA tres tipos de protocolos juegan un papel muy importante: protocolos de marcación telefónica como el PPP, los de seguridad como RADIUS y los de contraseña como CHAP. Los de marcación telefónica son protocolos de red que manejan señales a través de líneas telefónicas manteniendo unidos los paquetes IP entre el servidor de acceso y el usuario remoto. Los protocolos de seguridad proporcionan el sistema de mensajería cliente-servidor hacia la base de datos centralizada del usuario. Los protocolos de contraseña son mecanismos relativamente sencillos para manejar el inicio de sesión de las personas. Algunos protocolos de marcación telefónica incorporan su propio protocolo de contraseña (ARAP, por ejemplo).

Métodos y tipos de autorización de AAA AAA tiene siete métodos de autorización. En realidad son ocho, pero el método **none** es una solicitud para no llevar a cabo ningún procedimiento de autorización. En la tabla 6-3 se explican los métodos de autorización de AAA. Cada método es una palabra clave que se utiliza como argumento con el comando raíz **aaa authorization**. Éstos, a su vez, se aplican a los tipos de entidad asegurados.

Palabra clave del comando del IOS	Método de autorización de AAA
Group TACACS+	Envía un mensaje solicitando información de autorización desde el servidor TACACS+.
Group RADIUS	Envía un mensaje solicitando información de autorización desde el servidor RADIUS.
If-authenticated	Permite el acceso a la función solicitada si el usuario ya ha sido autentificado. (*If* aquí es la palabra *if*, que significa "depende de", y no el nemónico que el IOS utiliza para la interfaz de red en la solicitud config.)
Local	Utiliza la base de datos local del usuario para ejecutar el programa de autorización.

Tabla 6-3. Los ocho métodos con nombre de AAA para la autentificación del usuario (*continúa*).

Palabra clave del comando del IOS	Método de autorización de AAA
Krb5-instance	Utiliza una instancia definida en el mapa de instancias de Kerberos.
Cache *nombre del grupo*	Autoriza el uso de un grupo servidor de caché.
Group *nombre del grupo*	Autoriza el uso de un subconjunto de servidores RADIUS y TACACS+ para la contabilidad como está definido en el comando **server group** *nombre del grupo.*
None	No ejecuta ninguno de los métodos de autorización en este dispositivo de acceso.

Tabla 6-3. Los ocho métodos con nombre de AAA para la autentificación del usuario (*conclusión*).

Como ya se mencionó, RADIUS y TACACS+ pueden coexistir en el mismo dispositivo de acceso. En función de la conexión que se esté tratando de hacer y de la manera en que esté configurado el equipo, el cliente solicitará los servidores RADIUS o TACACS+, que son bases de datos de usuario independientes.

El comando **if-authenticated** pasa por alto la autorización si el usuario ya ha sido autentificado en algún otro lado. Esto es importante; durante una sola sesión, un usuario puede realizar docenas de conexiones con entidades aseguradas por la autorización AAA (como los modos de comando del IOS), y sería poco práctico para el dispositivo cliente, consultar el servidor TACACS+ o RADIUS cada vez.

En general, una base de datos local del usuario del dispositivo sólo contiene nombres de usuario y contraseñas. Recuerde que los dispositivos de red no cuentan con discos duros y éstos deben almacenar permanentemente información en la memoria NVRAM, que podría estar saturada debido al almacenamiento de la imagen de arranque del IOS y también por los registros diarios de la contabilidad de AAA. Por esto, las bases de datos locales del usuario no suelen contener autorizaciones de los usuarios. Por tanto, si un servidor de seguridad no estuviera disponible mientras un usuario inicia sesión, será muy probable que dicho usuario no pueda acceder a ninguno de los servicios configurados que requieren autorización. En la figura 6-12 se muestra cómo una base de datos local del usuario coexiste con la base o las bases de datos del servidor.

Si no se va a ejecutar ninguna autorización en la entidad segura, esto debe configurarse de manera explícita utilizando el comando **none**. De otra manera, el software del IOS automáticamente reforzará en forma predeterminada los métodos de autorización. Los cinco tipos de objetos seguros a los que se pueden aplicar los métodos de autorización de AAA, se explican en la tabla 6-4.

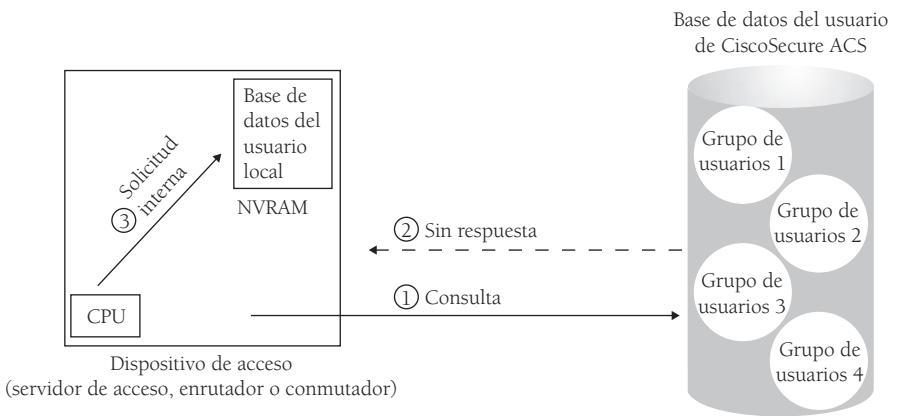


Figura 6-12. Una base de datos de usuario puede almacenarse en la NVRAM del dispositivo de acceso para su uso local.

Los cinco tipos de entidades de autorización pueden dividirse en dos pares:

- ▼ Cada uno de los métodos EXEC y Command tienen que ver con el acceso a los comandos del IOS.
- ▲ Los métodos Network y Reverse Access se relacionan con las conexiones, pero con las que operan en direcciones diferentes.

Como opción predeterminada, en los dispositivos de acceso de Cisco, el comando **aaa authorization config-commands** está habilitado. De esa forma, el dispositivo cuenta con seguridad en cuanto se saca de la caja, en caso de que el administrador lo instale sin configurar

Tipo	Tipo de autorización de AAA
Red	Aplica el método a las solicitudes de servicio relacionadas con la red, incluidas las conexiones de acceso directo (vía la consola o AUX), las Telnet (vía IP o IPX) o las de marcación telefónica (vía PPP, SLIP o ARAP).
Telnet Inverso	Aplica el método a las sesiones Telnet en que el usuario intenta conectarse desde un dispositivo de acceso seguro con otro host (una maniobra muy común de un hacker que ha ingresado a un dispositivo de red).

Tabla 6-4. Los cinco tipos de autorización del IOS (*continúa*).

Tipo	Tipo de autorización de AAA
EXEC	Aplica el método a sesiones en el modo de comando EXEC de usuario y puede aplicarse por usuario, por fecha, y por el tiempo de arranque y detenimiento.
Comandos	Aplica el método para restringir el acceso a comandos específicos. Los métodos del comando deben aplicarse a un grupo del IOS por comando. Existen dos grupos predeterminados: números 0 y 15 (modos EXEC de usuario y EXEC privilegiado, respectivamente). El método Command puede aplicarse al usuario por fecha y tiempos de arranque y detenimiento.
Configuración	Descarga la configuración del servidor AAA.

Tabla 6-4. Los cinco tipos de autorización del IOS (*conclusión*).

la seguridad. La siguiente instrucción de ejemplo ilustra un enrutador que se está configurando con el fin de solicitar autorización para conectarse a una red de cualquier tipo. Esto sería válido, por ejemplo, si la conexión se estableció mediante inicio de sesión a la TTY de la consola, un inicio de sesión a la VTY de Telnet o un inicio de sesión por marcado telefónico mediante PPP:

```
MyRouter(config)#aaa new-model
MyRouter(config)#aaa authorization network NetTeam group tacacs+ local
```

El comando anterior especifica que el protocolo de seguridad TACACS+ puede utilizarse para verificar usuarios contra la lista de métodos con nombre NetTeam y utilizar la base de datos local para copia de seguridad. Esta autorización se aplica en forma predeterminada a todas las interfaces de red en el dispositivo (al contrario de los métodos de autentificación, que deben aplicarse a líneas específicas).

Pero, como ya se mencionó, a veces no es práctico tener autorizaciones almacenadas en el dispositivo. Para resolver esto, la restricción podría hacerse menos severa utilizando el comando **none** para permitir una conexión de red si el servidor TACACS+ no responde:

```
MyRouter(config)#aaa authorization network NetTeam group TACACS+ none
```

En el comando anterior, la identidad del usuario debió haber sido ya autentificada con una contraseña para llegar hasta este punto en la configuración de AAA. El comando **none** sólo surte efecto cuando el servidor TACACS+ no responde. Las instrucciones siguientes configuran una autorización un poco más sofisticada:

```
MyRouter(config)#aaa authorization commands 15 SeniorTechs group TACACS+
MyRouter(config)#line vty 0 5
MyRouter(config-line)#authorization commands 15 SeniorTechs
```

Las instrucciones anteriores muestran un ejemplo de la configuración por línea, al contrario de la interfaz de red. Aquí están aseguradas las seis líneas (VTY) terminales virtuales. En este ejemplo, la lista de métodos con nombre SeniorTechs está declarada como necesaria para que un administrador utilice el nivel 15 de comandos del IOS en este dispositivo. Se mencionó antes que el comando **level** del IOS puede utilizarse para autorizar el uso de un grupo de comandos. Como opción predeterminada, todos los comandos en el modo Privileged EXEC están agrupados en el nivel 15 y todos los comandos en el modo User EXEC en el nivel 0. Por tanto, el fragmento de código anterior especifica que sólo a los administradores con los perfiles de usuario configurados con los atributos SeniorTechs se les permitirá utilizar los comandos en modo Privileged EXEC.

Métodos y tipos de contabilidad Los métodos de contabilidad de AAA configuran las actividades de los usuarios que se rastrearán dentro de un dispositivo de acceso seguro. Los métodos de contabilidad recopilan datos de los paquetes TACACS+ y RADIUS y los registran. En la tabla 6-5 se explica cómo funcionan los dos.

Observe que los únicos métodos de contabilidad son los propios protocolos de seguridad. Esto se debe a que la información de contabilidad es recolectada en forma predeterminada para todo el dispositivo. La razón de los dos métodos es que los datos de contabilidad deben circular en paquetes TACACS+ o RADIUS hacia el servidor (la contabilidad AAA no se realiza sin servidores).

AAA tiene seis tipos de entidades de contabilidad segura, ligeramente diferentes a las entidades de autorización. La tabla 6-6 las explica.

La palabra clave de contabilidad **system** sólo recolecta un conjunto de variables en forma predeterminada. No puede configurarse para recolectar sólo ciertos eventos. La razón es que un evento del sistema simplemente sucede (un usuario no solicita permiso para provocar que suceda). Un ejemplo de un evento del sistema sería una interfaz de red que dejara de trabajar a las 11:32:28 del jueves 9 de enero de 2007. La contabilidad AAA no asocia automáticamente el evento del sistema con una transacción de seguridad, pero al comparar los registros de autorización y contabilidad de esa fecha y hora facilitaría que un administrador de red tuviera una idea acerca de quién fue el culpable.

Palabra clave del comando	Método de contabilidad del AAA
TACACS+	Registra información de la contabilidad acerca de TACACS+ en la base de datos de CiscoSecure ACS.
RADIUS	Registra información de la contabilidad acerca de RADIUS en la base de datos de CiscoSecure ACS.

Tabla 6-5. Cómo funcionan los métodos de contabilidad de AAA por protocolo de seguridad.

Palabra clave del comando	Tipo de contabilidad de AAA
Red	Aplica el método a las conexiones de red, generalmente una conexión PPP, pero los métodos también pueden nombrarse para conexiones de inicio de sesión, SLIP y ARAP.
Auth-proxy	Proporciona información acerca de todos los eventos de usuario autentificados por proxy.
EXEC	Proporciona información acerca de todas las sesiones terminales en el modo User EXEC dentro del ambiente IOS del dispositivo de acceso. La información de contabilidad del EXEC puede recolectarse por usuario, fecha y horas de inicio y detención.
Comandos	Proporciona información acerca de cualquier comando generado por los usuarios que sean miembros de un modo Privileged EXEC del IOS. La información de contabilidad de comandos puede recolectarse por usuario, fecha y horas de inicio y detención.
Conexión	Proporciona información acerca de todas las conexiones salientes que se intentaron desde el dispositivo de acceso seguro en sesiones que utilizaron protocolos de terminales Telnet, rlogin, TN270, PAD y LAT.
Sistema	Proporciona información acerca de eventos en el sistema como los reinicios.

Tabla 6-6. Tipos de contabilidad de AAA que rastrean el uso de activos para cinco tipos de entidades de seguridad.

Como en el caso de la autorización, se deben aplicar listas del método de nombrado de la contabilidad AAA a todas las interfaces de red que se desea asegurar y, después, se debe aplicar a un tipo de contabilidad indicado. Por ejemplo, el comando MyRouter(config)**#aaa accounting network group** *nombre del grupo* **TACACS+** configura el IOS para que lleve un registro de todas las conexiones SLIP y PPP hechas en una interfaz de red que tiene autorización para utilizar el TACACS+.

La contabilidad es un poco más complicada en la forma como registra las solicitudes. La contabilidad AAA depende de las noticias de contabilidad para recolectar datos. Una *noticia de contabilidad* es un paquete especial que notifica el método de contabilidad de un evento. Esta información se almacena en el archivo de registro de contabilidad para cargarse en el servidor de seguridad apropiado. Se debe utilizar una de tres palabras clave de la contabilidad de AAA para especificar exactamente cuándo se van a enviar las noticias durante el proceso de solicitud del servicio. La terminología puede ser un poco confusa, pero la figura 6-13 le ayudará a visualizar cómo funcionan las tres:

- ▼ **Sólo detención** Para contabilidad mínima. Hace que RADIUS o TACACS+ envíen una noticia de detener la grabación de los datos de contabilidad al *final* del servicio solicitado. La contabilidad de sólo detención es buena únicamente para rastrear quién fue a qué lugar. Ésta es información importante para efectos de seguridad.
- ■ **Inicio-detención** Para más contabilidad. Hace que RADIUS o TACACS+ envíen una noticia de inicio de la contabilidad al *comienzo* del servicio solicitado y una noticia de detención de la contabilidad al final del servicio. La contabilidad inicio-detención proporciona el tiempo transcurrido de una conexión.
- ▲ **Espera-inicio** Para máxima contabilidad. Hace que RADIUS o TACACS+ esperen hasta que la noticia de inicio reciba la contabilidad AAA *antes* de que comience el proceso de solicitud del usuario. La mayoría considera que la espera-inicio es una exageración y una inconveniencia para los usuarios, por lo que su uso está limitado a servicios muy sensibles. Se utiliza en versiones antiguas del IOS.

Para seleccionar un método, incluya cualquiera de las tres palabras clave como argumentos del comando raíz **aaa accounting** en la instrucción de la configuración. Las tres opciones proporcionan diferentes niveles del control de la contabilidad. Por ejemplo, si un administrador solicita el ingreso a un modo User EXEC de un dispositivo seguro, el proceso de sólo detención únicamente registra el final de la sesión del administrador dentro del modo User EXEC. El proceso inicio-detención registra el inicio y el final de la sesión. El proceso espera-inicio asegura que no se realice ninguna conexión antes de que la noticia de la contabilidad haya sido recibida y confirmada.

- ▼ **none** Sin contabilidad.
- ■ **start-stop** El registro inicia y se detiene sin esperar.
- ▲ **stop-only** El registro se detiene cuando termina el servicio.

El siguiente ejemplo muestra una configuración de la contabilidad AAA. Las líneas 2, 3 y 4 muestran las tres funciones AAA que se configuran simultáneamente, lo que es una práctica muy común.

```
MyAccessServer(config)#aaa new-model
MyAccessServer(config)#aaa authentication login NetTeam local
MyAccessServer(config)#aaa authentication ppp RemoteWorkers group TACACS+ local
MyAccessServer(config)#aaa authorization network NetTeam group TACACS+ local
MyAccessServer(config)#aaa accounting network WeWillBillYou none
```

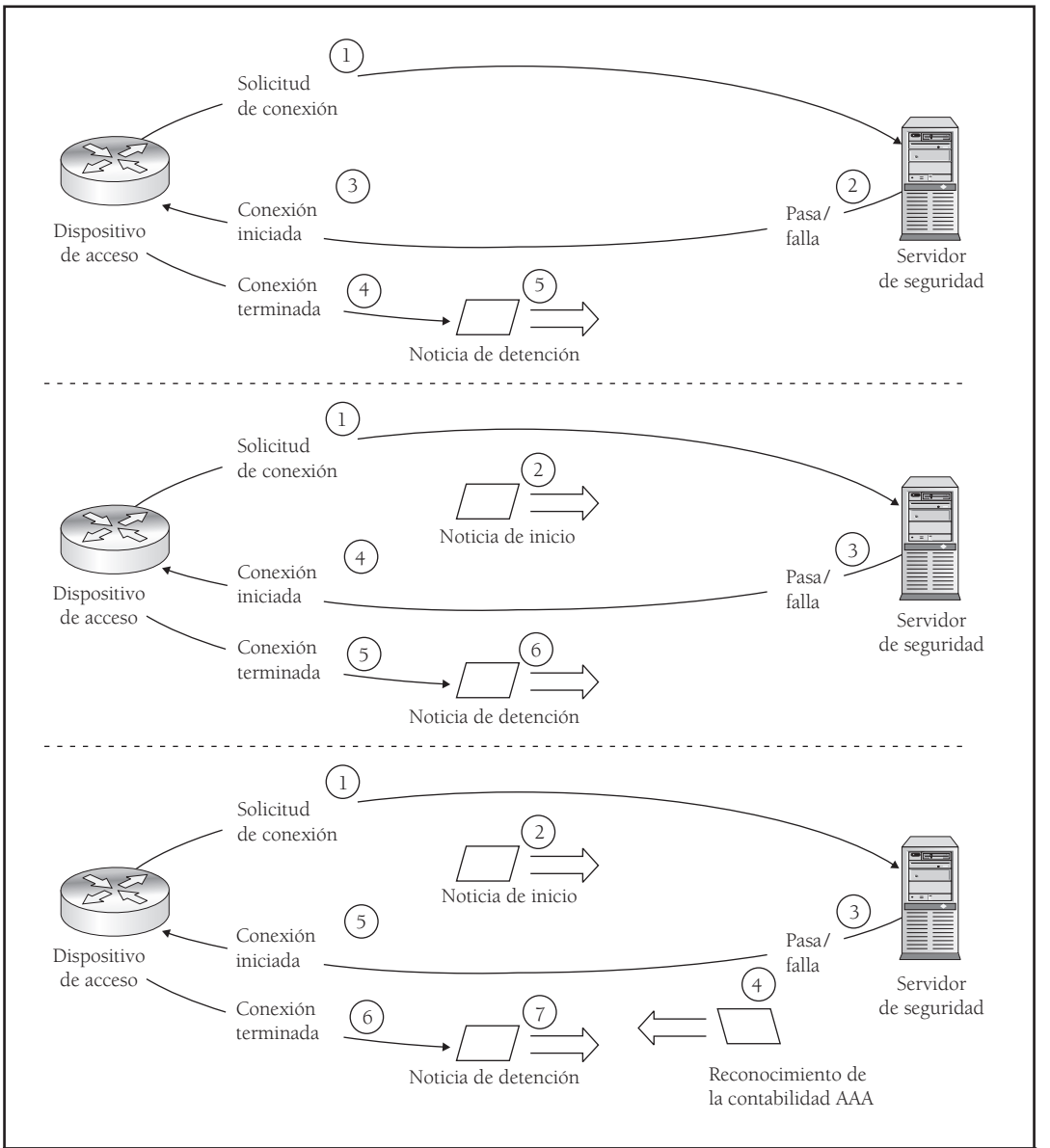


Figura 6-13. La contabilidad AAA puede utilizar cualquiera de los tres métodos para rastrear la actividad del usuario.

```
MyAccessServer(config)#
MyAccessServer(config)#tacacs-server host BigUnixBox
MyAccessServer(config)#tacacs-server key JustBetweenUs
MyAccessServer(config)#
MyAccessServer(config)#interface group-async 1
MyAccessServer(config-if)#group-range 1 16
MyAccessServer(config-if)#encapsulation ppp
MyAccessServer(config-if)#ppp authentication chap RemoteWorkers
MyAccessServer(config-if)#ppp authorization NetTeam
MyAccessServer(config-if)#ppp accounting WeWillBillYou
```

Los comandos de contabilidad están entrelazados con los demás para darle una idea del aspecto real de las instrucciones. Como se configuró aquí, los registros totales de la contabilidad inicio-detención se asentarán para todas las conexiones de red realizadas por el equipo de red a través de cualquiera de los 16 puertos asincrónicos del dispositivo, MyAccessServer.

Lo que se registra depende exactamente de la manera en que la lista de métodos con nombre WeWillBillYou esté configurada. La mayoría de los administradores de red, por lo menos, usarían el comando **network** para llevar un registro de los tiempos de conexión. En general, los parámetros orientados a comandos **exec** y **commands** sólo son útiles para auditorías de seguridad.

Atributos de RADIUS y TACACS+

Un protocolo de seguridad se define en gran medida por los atributos que soporta. Después de todo, las herramientas de seguridad definen la materia prima que se utiliza para operar los sistemas de seguridad basados en el usuario. RADIUS y TACACS+ son protocolos independientes empaquetados en una estructura de comandos AAA dentro del IOS. Las diferencias principales entre los dos se hacen presentes dentro de la base de datos del usuario, donde cada usuario tiene un perfil de seguridad que contiene los atributos que definen qué puede hacer una persona determinada. Como tecnologías independientes, RADIUS y TACACS+ tienen sus propios atributos.

RADIUS es un estándar abierto bajo los auspicios del IETF y define casi 60 atributos. No los presentaremos aquí, pero en la tabla 6-7 se muestran algunos con ayuda para ver los elementos relacionados con la seguridad basada en el usuario.

Diecisiete atributos de RADIUS se conocen como atributos que son propiedad de los fabricantes. Se trata de artículos que los fabricantes pueden diseñar a la medida para extender la funcionalidad de sus productos. En la tabla 6-8 se muestran algunas extensiones de Cisco para darle una idea de lo que le gusta personalizar a los fabricantes.

TACACS+ cuenta con más de 50 atributos (pares atributo-valor). Aunque TACACS+ y RADIUS soportan las tres funciones AAA, TACACS+ es más sofisticado. Por ejemplo, posee atributos como el Túnel-ID para ayudar a asegurar conexiones VPN. Ésta es la razón por la que las interconexiones que utilizan RADIUS para autenticar a los usuarios de marcación telefónica a menudo utilizarán TACACS+ para autorización y contabilidad. En la tabla 6-9 se muestran atributos TACACS+ de ejemplo para darle una idea del protocolo.

La muestra de pares AV de la tabla 6-9 presenta dos áreas en que TACACS+ es más robusto que RADIUS. En primer lugar, TACACS+ ofrece seguridad interna más estricta

Atributo de RADIUS	Descripción
User-Name	El nombre de la cuenta con el perfil del usuario de una persona. Por ejemplo, el nombre de usuario de Ana Rosa podría ser "arosa".
User-Password	El código de acceso secreto creado por la persona.
CHAP-Password	El valor codificado que el sistema regresa durante el intercambio de saludo con desafío. Es el nombre del usuario mezclado con un número aleatorio llamado *desafío*.
NAS-IP Address	La dirección IP del servidor de acceso que solicita la autentificación. (Recuerde que NAS son las siglas de Network Access Server: servidor de acceso a la red.)
NAS-Port	El número de puerto físico en el servidor de acceso. Esto incluye los diferentes tipos de posibles interfaces, como líneas de terminal asincrónicas, líneas de red sincrónicas, canales ISDN y otros tipos de interfaces.
Service-Type	El servicio solicitado u otorgado (por ejemplo, un administrador puede solicitar el comando **enable** en el IOS para ingresar al modo de comando Privileged EXEC).
Login-Port	El puerto TCP con el que el usuario se va a conectar (por ejemplo, el puerto 80 para la navegación Web HTTP).
Acct-Session-ID	Un identificador único de contabilidad utilizado para comparar noticias de arranque y detención en un archivo de registro de la contabilidad.
Acct-Session-Time	El número de segundos que el usuario permaneció conectado.
Acct-Authentic	La manera en que el usuario fue autentificado, ya sea por RADIUS, por la bases de datos local del usuario, por TACACS+ o por Kerberos.

Tabla 6-7. Los atributos de RADIUS utilizados para imponer la seguridad basada en el usuario.

que RADIUS, poniendo candados a los comandos y listas de acceso. La primera acción que un hacker haría una vez que entrara a un dispositivo IOS sería ingresar nuevos parámetros en sus listas de acceso, lo que permitiría transferencias de archivos. Estos pares AV no sólo ayudan a detener a los intrusos, sino que también permiten que el administrador de la red especifique con qué dispositivos, comandos del IOS o listas de acceso pueden trabajar los administradores individuales. Prohibir el acceso a ciertos miembros de grupos ayuda a evitar la comisión de errores de configuración.

Atributo de RADIUS específico de Cisco	Descripción
Password-Expiration	Especifica un intervalo de tiempo o un evento que obliga al usuario a crear una nueva contraseña.
IP-Direct	El dispositivo de Cisco hará caso omiso de todas las tablas de enrutamiento y enviará los paquetes directamente a una dirección IP específica. Por ejemplo, el IP-Direct puede utilizarse para asegurarse de que una conexión WAN de un usuario pase a través de un firewall.
Idle-Limit	Especifica el número máximo de segundos que una sesión puede estar inactiva.

Tabla 6-8. Las extensiones de Cisco del estándar RADIUS.

La segunda área en que TACACS+ es más fuerte, es el soporte de protocolos. Por ejemplo, TACACS+ cuenta con pares AV para mejorar la seguridad de VPN, que se están haciendo muy populares. Como se esperaría, TACACS+ también cuenta con atributos de contabilidad para equipararse a las áreas donde se expande más allá del RADIUS. Por ejemplo, el par AV **cmd5*x*** le permite conservar un registro de los comandos de IOS que utiliza un administrador, mientras trabaja con un dispositivo. Esta información sería de gran utilidad para diagnosticar cómo se cometió un error de configuración.

Par AV del TACACS+	Descripción
service*5x*	Especifica el servicio de conexión que se va a autorizar o registrar. Por ejemplo, **aaa authorization service-5ppp** se utilizaría para autorizar a una persona a que efectúe una conexión PPP remota con un dispositivo. Otro ejemplo sería **service5shell** para permitir que un administrador ingrese al modo de comando Privileged EXEC de un dispositivo.

Tabla 6-9. Pares AV de autentificación y autorización del TACACS+ (*continúa*).

Par AV del TACACS+	Descripción
protocol*5x*	Un protocolo es un subsistema de un servicio. Por ejemplo, una conexión PPP podría utilizar TN3270, VINES, Telnet u otros protocolos. Un protocolo clave en estos días es VPDN (Virtual Private Dialup Network, red privada virtual de marcación telefónica). El par AV **protocol5vpdn** permite que un usuario de marcación telefónica remota establezca una conexión codificada con la VPN de la compañía.
routing*5x*	Especifica si las actualizaciones de enrutamiento pueden propagarse por medio de la interfaz utilizada para la conexión.
priv-1v1*5x*	Especifica el modo de comando del IOS que puede usar la persona. Para que esto funcione, primero deben agruparse los comandos utilizando el comando **level**.
acl*5x*	Restringe las listas de acceso a la conexión en un dispositivo. Las listas de acceso a la conexión también se llaman *listas de acceso reflexivo* y se utilizan para rastrear sesiones.
inacl*5x*, inacl#*5x*, outacl*5x*, outacl#*5x*	Cuatro pares AV que restringen el acceso a listas de acceso entrantes y salientes por usuario que residen en una interfaz.
tunnel-id	Especifica el nombre del usuario para establecer conexiones VPN remotas.
gw-password*5x*	Especifica la contraseña que reside en la gateway doméstica de la VPN. Debe utilizarse con **service5ppp** y **protocol5vpdn**.

Tabla 6-9. Pares AV de autentificación y autorización del TACACS+ (*conclusión*).

LISTAS DE ACCESO DINÁMICO

Echémosle un vistazo rápido a las listas de acceso en cuanto a la forma como se relacionan con TACACS+ y RADIUS. Las listas de acceso suelen utilizarse para filtrar el tráfico en el paquete. En otras palabras, cuando se intenta una conexión a través de una interfaz de un enrutador, se inspeccionan los encabezados de los paquetes para ver si éstos tienen direcciones IP o números de puertos de aplicación prohibidos, y el tráfico se deja pasar o se bloquea. A éstas se les llama listas de acceso extendidas y se estudian en el capítulo 7. Para revisarlas aquí, dichas listas de acceso son *extendidas*, en el sentido de que pueden filtrar con base en los números de puerto de la aplicación de la red en lugar de sólo las direcciones. También

se les llama listas de acceso extendido *estáticas*, porque los comandos **permit** y **deny** son impuestos a ciegas, sin considerar al usuario. Para hacer una excepción con una persona en particular, el administrador tiene que acceder al archivo config del enrutador y editar la lista para esa interfaz.

Las listas de acceso dinámico se configuran utilizando los comandos conocidos como de cerradura y llave. Mediante éstos, se le puede otorgar a un usuario, que de otra forma sería bloqueado, acceso temporal a una red o subred a través de una sesión Telnet por Internet.

La sesión Telnet está abierta a un enrutador configurado para cerradura y llave. La lista de acceso dinámico solicita al usuario el ingreso de información de autentificación. Así como igual que con los demás protocolos de seguridad basados en el usuario, puede configurarse la apertura y cierre para comparar con la base de datos del usuario en el propio enrutador (local) o con la base de datos del usuario que se conserva en el servidor TACACS+ o RADIUS. Si procede la autentificación, se saca al usuario de la sesión Telnet y puede iniciar una aplicación normal, como un navegador.

Cerradura y llave con una base de datos local de usuario

La secuencia siguiente de fragmentos de código muestra cómo puede configurarse la cerradura y llave en un enrutador, mediante un archivo de autentificación del usuario mantenido localmente. Para comenzar, se declara una interfaz particular de red en el enrutador, junto con una dirección IP de subred. El comando **ip access-group** pone bajo el control de la lista de acceso 103 a la interfaz apenas nombrada y a las redes:

```
MyRouter(config)#interface ethernet1
MyRouter(config-if)#ip address 209.198.208.30 255.255.255.0
MyRouter(config-if)#ip access-group 103 in
```

La palabra clave **in** especifica que el control de acceso se aplique solamente a conexiones entrantes (la cerradura y llave también puede utilizarse para restringir conexiones salientes).

En la instrucción siguiente, la primera entrada 103 de la lista de acceso sólo permite conexiones Telnet en el enrutador. La segunda entrada 103 es ignorada hasta que la cerradura y llave se dispare siempre que se haya establecido una conexión Telnet en el enrutador. La palabra clave **dynamic** define la lista de acceso 103 como una lista dinámica (cerradura y llave).

```
MyRouter(config)#access-list 103 permit tcp any host 209.198.207.2 eq
telnet
MyRouter(config)#access-list 103 dynamic InCrowd timeout 60 permit ip
any any
```

Ésta es la unión clave. Si se configura de esa manera, el intento de conexión Telnet hacia el enrutador causa que lo compare con su base de datos local para ver si el usuario y la contraseña son válidos para el acceso de cerradura y llave al enrutador. Si es válida, la instrucción **timeout 60 permit ip any any** proporciona al usuario 60 minutos para usar el enrutador como una conexión entre cualquier par de direcciones IP.

Por último, una instrucción **autocommand** genera una lista de acceso entrante temporal (llamada InCrowd en la instrucción anterior) en la interfaz de red Ethernet1 y la línea 0 en el enrutador. La instrucción con la lista de acceso temporal expirará después de cinco minutos.

```
MyRouter(config)#line vty 0
MyRouter(config-line)#login local
MyRouter(config-line)#autocommand access-enable timeout 5
```

La instrucción con la lista de acceso temporal no se elimina automáticamente cuando los usuarios terminan la sesión. Permanecerá configurada hasta que expire el periodo.

Las listas de acceso dinámico también pueden configurarse para autentificar a los usuarios, comparándolos con la base de datos mantenida en el servidor TACACS+ o RADIUS. Esto, en efecto, convierte a un enrutador en un servidor de acceso mediante el cual un usuario puede acceder a una interconexión pero sólo registrándose mediante una sesión Telnet.

Está de más decirlo y, en efecto, se trata de un cliché: la seguridad de la red es importante y necesaria en extremo. Sin embargo, una cosa es comprender que es importante y otra entender cómo implantarla en la realidad. Para estar seguro de esto, puede escribirse un libro completo (y de hecho muchos) sobre el tema de la seguridad en las redes en general y de la seguridad de Cisco en particular. El objetivo de este capítulo fue mostrarle diferentes detalles que se encuentran detrás de algunos componentes importantes que sirven para asegurar su interconexión. En el capítulo 7, hablaremos acerca de algunas herramientas específicas que Cisco ofrece en el mundo del acceso a redes y seguridad.

CAPÍTULO 7

Los bloques de construcción de la seguridad

En los capítulos anteriores vimos cómo se mueven los datos por las interconexiones. Comienza en el cable de par trenzado que opera desde el escritorio. Después, vemos a los mensajes que circulan entre concentradores, conmutadores y enrutadores. De manera muy rápida, los datos llegan a su destino a través de los edificios o al otro lado del mundo. Toda esta tecnología ha hecho posible cosas asombrosas. En la actualidad es algo muy común que los negocios vendan y proporcionen soporte a toda una línea de productos desde los sitios Web (algo impensable hace una década). Igualmente impresionante es que se esté administrando a compañías completas dentro de plataformas de administración de interconexiones. Hasta es posible operar redes privadas a través de Internet público. Pero hay una trampa en toda esta tecnología: las redes son carreteras de doble sentido. Si pueden pasar cosas positivas en una interconexión, se puede deducir que también pueden suceder cosas negativas.

La conexión de una computadora a cualquier tipo de red conlleva un riesgo, necesariamente. Conectar a toda una empresa, como puede imaginar, plantea una gran cantidad de problemas relacionados con la seguridad. La seguridad en las redes es un tema muy amplio que incluye directivas, guardias de seguridad, técnicas, estándares, protocolos, algoritmos y productos especializados de hardware y software. La seguridad ha sido fundamental en el área de la computación desde los tiempos de los mainframes centrales y las terminales con pantallas en color verde. En la actualidad, los expertos consideran que la seguridad es el obstáculo más grande para que Internet se convierta en el entorno de negocios que abarca todo y en el que todos hemos pensado. En realidad, la seguridad es tan importante que existe toda una industria dedicada a ella.

Lograr una buena seguridad es algo muy difícil, debido a que los sistemas están muy interconectados. En los viejos tiempos se contaba con una terminal conectada al mainframe o se estaba perdido. Pero en esta era de la conectividad, cualquier persona que tenga los recursos y el tiempo suficientes puede entrar a cualquier sistema que esté conectado a Internet. La vulnerabilidad es un hecho en el campo de la conectividad y la respuesta de la industria es un pelotón de tecnologías de seguridad.

Toda seguridad comienza con el *acceso*. Aun en los días de los hombres de las cavernas, contar con una buena seguridad significaba no permitir la entrada a cosas malas ni la salida a cosas valiosas. La interconectividad no es diferente. Operar una interconexión es como administrar un negocio: quiere que los extraños entren libremente a su negocio, pero eso inevitablemente significa darles oportunidad a los ladrones y vándalos de que vean lo que hay en su tienda. Tiene que mantener abierto el acceso a su negocio; todo lo que debe hacer es tratar de eliminar a los chicos malos. Existen tres tecnologías de acceso a las redes que tratan de equilibrar las necesidades en conflicto de acceso y seguridad:

- ▼ **Firewalls** Son enrutadores especiales que interceptan y controlan el tráfico entre una red privada y las redes públicas (especialmente Internet).
- ■ **Redes privadas virtuales (VPN, Virtual Private Networks)** Son redes privadas que operan sobre una red pública (generalmente Internet).
- ▲ **Dispositivos de acceso** Son dispositivos dedicados que se utilizan para conectar usuarios remotos a las interconexiones mediante Internet o líneas telefónicas normales. Dentro de estos productos se incluyen los servidores y enrutadores de acceso.

De estas tres tecnologías, sólo el firewall está avocado a la seguridad, y no proporciona tanto acceso como lo permite. Las otras dos (VPN y los servidores de acceso) existen principalmente para entregar conectividad eficiente. Los servidores de acceso permiten que personas ubicadas remotamente puedan ingresar a las interconexiones. La misión de una VPN es operar una red de área amplia (WAN) sobre Internet, pero tanto los servidores de acceso como las VPN restringen los accesos no autorizados e intentan asegurar la integridad de los datos.

NOTA No hablaremos específicamente de los servidores de acceso en este capítulo. Lo importante es saber que estos dispositivos se utilizan para acomodar el acceso por marcado telefónico. Los usuarios de este tipo de acceso llaman a la red y se conectan a ella utilizando el banco de módems del servidor de acceso. Una vez que han sido autentificados, pueden acceder a los recursos de la interconexión. En este capítulo se estudian las tecnologías de acceso de Cisco desde las perspectivas de la función y la seguridad.

FIREWALLS

Un *firewall* es un punto de control de tráfico entre una red privada y una o más redes públicas. Es una compuerta que decide de manera selectiva qué puede entrar o salir de una red protegida. Para hacer esto, el firewall debe ser la única compuerta entre la red que protege y el mundo exterior. Si el tráfico puede evitar un firewall, la seguridad que éste ofrece no vale nada. Un principio básico es que todo el tráfico entrante y saliente debe pasar por el firewall. Un enrutador normal podría servir como firewall rudimentario si estuviera configurado como un punto de estrangulamiento. En la figura 7-1 se muestra cómo un firewall actúa como un conducto a través del cual debe circular todo el tráfico.

Debe haber necesariamente un equilibrio entre la seguridad y el desempeño de la red. Si sustituye los autos y los camiones por paquetes IP en la figura 7-1, verá que el tráfico proveniente de varias supercarreteras confluirá en una sola rampa. Si la seguridad no fuera una preocupación, para mejorar el desempeño, las interconexiones privadas estarían rodeadas por todos lados de enrutadores.

Fundamentos de los firewalls

En términos muy simples, un firewall funciona como un filtro de tráfico. Éste ingresa al firewall a través de una interfaz de red y lo abandona a través de otra, y en firewalls básicos, los mensajes se manejan en el nivel de la capa de red (capa 3) de las siete capas del modelo OSI. Los firewalls de la más alta seguridad para el filtrado de aplicación manejan los mensajes y los filtran también en la capa 7.

Los firewalls operan interceptando e inspeccionando cada paquete que entra a cualquiera de sus interfaces de red. Las inspecciones varían de acuerdo con la sofisticación del firewall y de lo estricta que sea la política de seguridad. Pero el objetivo es siempre identificar una coincidencia entre el contenido de cada uno de los paquetes y las reglas de seguridad con que el firewall ha sido programado para imponer. Los pasos fundamentales de la intercepción e inspección de paquetes se muestran en la figura 7-2.

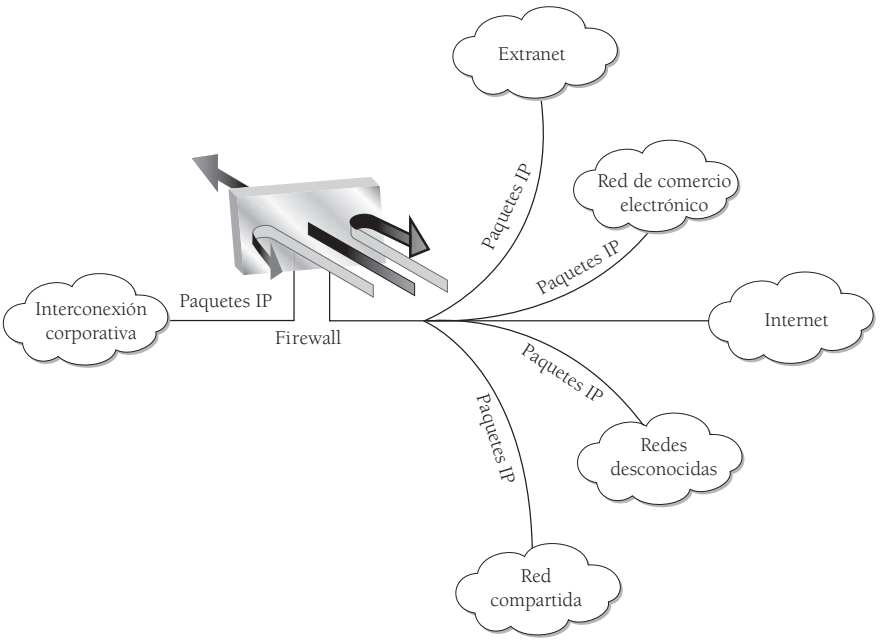


Figura 7-1. Un firewall se define parcialmente por su posición como cuello de botella.

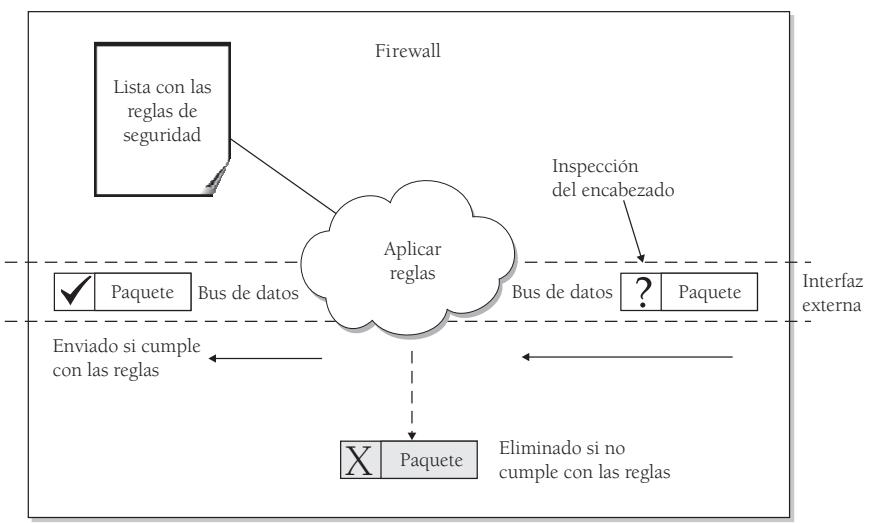


Figura 7-2. Los firewalls inspeccionan todos los paquetes y les aplican las reglas de seguridad.

No hay nada extravagante en la manera en que un firewall intercepta el tráfico. Lo hace al llevar todo el tráfico que entra a sus interfaces de red a través de una sola trayectoria (llamada *bus de datos* en terminología computacional). Al hacer que todo el tráfico pase por el bus de datos interno y la memoria del firewall, al software que funciona en la Central Processing Unit (CPU, unidad de procesamiento central) se le brinda la oportunidad de comprobar que cada paquete cumpla con las reglas de seguridad con las que el firewall ha sido programado para imponer.

La inspección real la hace un firewall de filtrado de paquetes al leer el encabezado del paquete para ver si las condiciones coinciden con las reglas establecidas en las tablas de seguridad. Por lo general, éstas incluyen docenas de reglas, cada una diseñada para aceptar o rechazar explícitamente tipos de tráfico específicos mediante la aplicación de una prueba de aceptado/rechazado a cada paquete. Si el paquete es aceptado, se envía a su destino. Si es rechazado, se elimina en la interfaz de red y deja de existir.

Los firewalls proyectan un panorama defensivo

Los enrutadores tienden a ver la vida en forma positiva. Se concentran en las direcciones y las mejores rutas para la entrega de mensajes. En contraste, los firewalls tienen una visión militarizada de las cosas, donde las direcciones aún son importantes, pero se usan para inspección y aceptación; no para entrega. Los firewalls definen el mundo dentro de las redes o fuera de ellas, haciendo la división de acuerdo con lo que hay más allá del perímetro de seguridad. Éste lo establecen uno o más firewalls ubicados entre la red segura y el mundo exterior. El firewall coloca a cada red que se encuentra a su paso en una de las tres clasificaciones siguientes:

- ▼ **Red de confianza** Reside dentro del perímetro de seguridad y se encuentra totalmente bajo el control administrativo de la empresa.
- ■ **Red insegura** Reside fuera del perímetro de seguridad y es conocida por el firewall, pero está más allá del control administrativo de la empresa.
- ▲ **Red desconocida** Es una red de la que el firewall no ha recibido ninguna información ni instrucciones, esto incluye casi todo Internet. Desde luego, las redes desconocidas son redes inseguras.

El perímetro de seguridad se dibuja justamente debajo de la mitad del firewall, y la configuración física del dispositivo como tal define lo que es interno y externo. Las interfaces de la red en el firewall están designadas como interfaces internas (*dentro*), externas (*fuera*) y *DMZ* (en algunos casos). A su vez, la red conectada a cada interfaz toma su designación de interfaz. Por ejemplo, en la figura 7-3, la red 10.1.13.0 está conectada a una interfaz interna y, por tanto, se define como dentro del perímetro de seguridad, por lo que se trata de una red de confianza.

En términos de seguridad en redes, el *control administrativo* es la capacidad para realizar tareas como la asignación de direcciones IP, la generación de cuentas de usuario y contraseñas y el mantenimiento de los archivos de configuración del dispositivo de la red. En general, el medio de la red (LAN y WAN) en que trabaja una red segura es propiedad de la empresa y está controlado por ésta. La excepción más significativa es la VPN, que opera principalmente a través de segmentos de red intermedios que son operados por alguien más; sin embargo, aún son consideradas como redes de confianza.

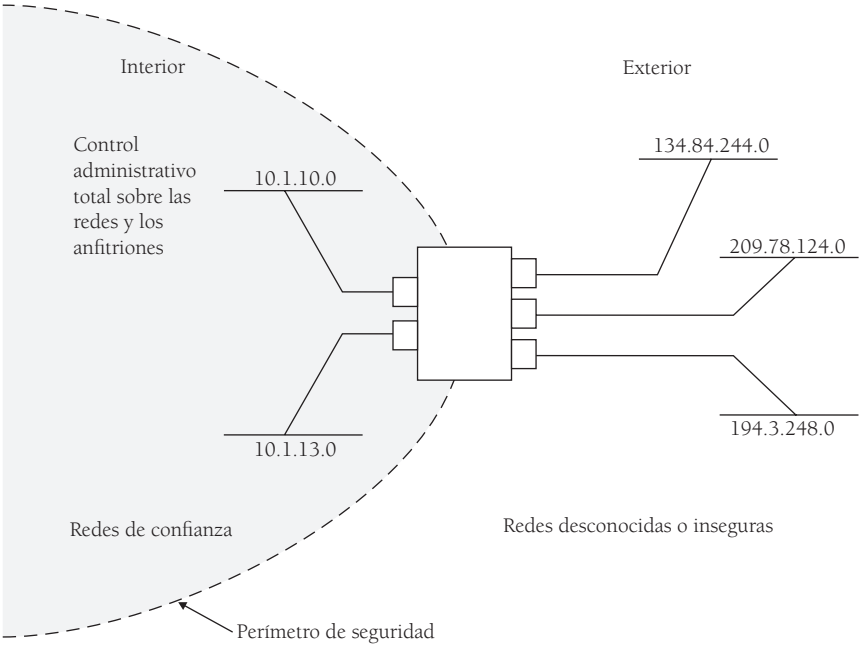


Figura 7-3. Los firewalls definen los perímetros de seguridad y clasifican las redes de acuerdo con éstos.

La seguridad es una cuestión de directivas y no de tecnología

La seguridad en las interconexión no se relaciona sólo con cuánto control pueda ejercer; también es importante cuánto control decida ejercer. De manera muy similar al intercambio entre seguridad y desempeño, existe también un equilibrio entre seguridad y conectividad. En teoría, cualquier LAN puede tener una postura de seguridad impenetrable externa, simplemente al desconectar todos los enrutadores, conmutadores y módems que lleven fuera la información.

Pero las empresas están obligadas a conectarse al mundo exterior porque los beneficios de la conectividad superan los riesgos que conlleva. En realidad, casi todos los negocios están conectados a la red pública más peligrosa y desconocida de todas: Internet. Cada vez que accede al sitio Web de una compañía para buscar información, descargar software o generar una orden de compra, dicha compañía ya ha tomado un riesgo calculado al dejarlo entrar a alguna parte de su sistema. Casi todas las compañías necesitan abrir sus redes internas al público, al menos hasta cierto punto. Los negocios lo hacen para vender y brindar soporte, los gobiernos para dar servicio y las organizaciones educativas para enseñar. Los firewalls tratan de ayudar a acomodar este compromiso de seguridad intencional definiendo una zona intermedia llamada *zona desmilitarizada* o DMZ, para abreviar. En la figura 7-4 se muestra una configuración típica de una DMZ.

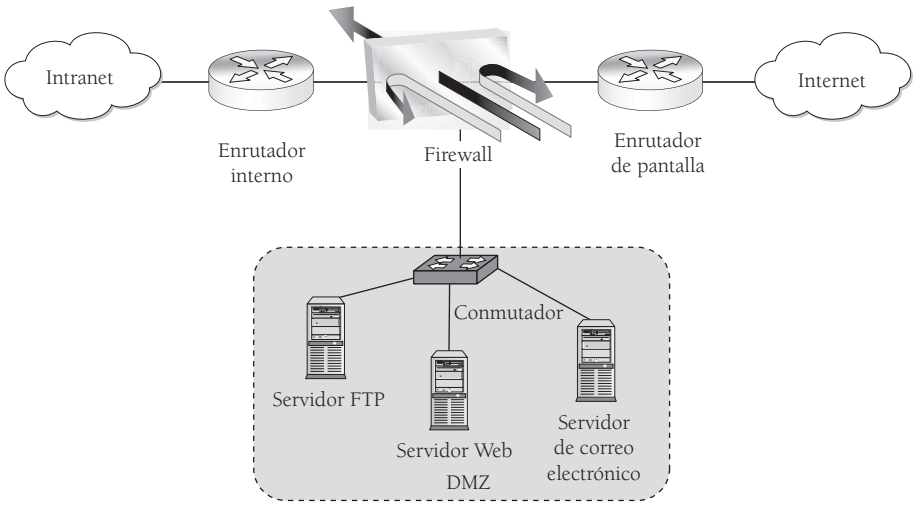


Figura 7-4. Muchas configuraciones de firewall incluyen una DMZ para operar servidores públicos.

A los segmentos LAN fuera del firewall se les llama *redes perimetrales externas*; a las de dentro, *redes perimetrales internas*. En general, cada red perimetral tiene conectado un enrutador y las listas de acceso suelen configurarse para bloquear parte del tráfico "malo". Sin embargo, a gran parte de este tráfico se le permite viajar hacia el firewall, donde puede hacer su trabajo de inspeccionar el tráfico contra intentos maliciosos y para llevar a cabo su función de imponer la ley de "bloquear o permitir" con base en las reglas definidas en el firewall. Al enrutador externo suele conocérsele como enrutador de *pantalla* o *escudo*; por lo general, tiene un proveedor de servicio de Internet (ISP) conectado al menos a una de sus interfaces. Además de la tarea de Internet a intranet, se necesita uno o varios firewalls para proteger a los servidores de la DMZ de un ataque y para restringir los permisos de conexión de esos servidores en la intranet. El punto clave que hay que comprender aquí, es que un firewall es una parte crítica de un ambiente seguro, que está diseñado para proteger a la intranet y la DMZ de tráfico malicioso y para imponer reglas de seguridad específicas definidas por su propietario (o administrador).

Cómo funcionan los firewalls

Las reglas de seguridad pueden definirse de manera global de manera tal que se apliquen a todo el firewall, además de que se pueden definir y aplicar otras reglas más específicas a una interfaz de red en particular. Esto es válido si el firewall es un enrutador que trata de servir como firewall o si es un dispositivo dedicado de alta tecnología, como el Firewall PIX de Cisco o el ASA de Cisco. Hablando de forma general, cada paquete o flujo se inspecciona y después se filtra con base en las reglas que se aplican a la tarjeta de interfaz de red especí-

fica, a través de la cual el paquete ingresó al firewall. Entonces, para configurar un firewall se debe, en gran medida, asignar reglas de seguridad a cada interfaz del firewall.

La lista de acceso es la herramienta más básica para la seguridad de las interconexiones

La forma más simple de tecnología de seguridad de redes es la lista de acceso. No se parece mucho a un firewall, pero aún es útil en una gran variedad de situaciones. También llamada *Access Control List* (*ACL, lista de control de acceso*) o *filtro*, la lista de acceso es un componente básico de cualquier configuración de firewall. Como su nombre lo indica, la lista de acceso restringe el acceso a la red a cierto tráfico. Proporciona un nivel básico de seguridad en la red filtrando los paquetes de acuerdo con estos criterios:

- **Direcciones IP de origen y destino** Son las direcciones IP en que se originó el paquete y a la que está dirigido.
- **Números de puerto de origen y destino** Son los números de puerto en que se originó el paquete y al que está dirigido.
- **Números de protocolo de origen y destino** Son los números de protocolo en que se originó el paquete y al que está dirigido.

Cisco las llama *listas de acceso extendido*: la extensión es el número de puerto, el número de protocolo (origen, destino, o ambos), la dirección IP de destino, o una combinación de todas ellas. Productos anteriores de Cisco sólo usaban las direcciones de origen, a las que se les conocía como listas de acceso estándar. Pero no se confunda con esta terminología; las *listas de acceso extendido* son el tipo básico de listas de acceso que se están utilizando en la actualidad.

NOTA Los números de puerto (también llamados puertos de red o tan sólo puertos) no son puertos físicos de interfaz como el S0 o E3. Los mensajes enviados por medio de los protocolos de la capa de transporte (capa 4), TCP o UDP, utilizan los números de puerto para identificar el protocolo de aplicación que va a operar la transmisión. Por ejemplo, el número para HTTP (WWW) es el puerto 80; el puerto de SMTP es el 25; y los de FTP son el 20 y el 21.

Los administradores de red crean listas de acceso en el archivo de configuración del enrutador. Se crea una lista de acceso por cada interfaz de red. Si una interfaz maneja el tráfico en varios protocolos de red (por ejemplo, IP, IPX y AppleTalk), cada protocolo de red tiene su propio formato de lista de acceso. Por tanto, se debe diseñar una lista de acceso independiente para que cada protocolo funcione en esa interfaz de red. Sin tomar en cuenta el protocolo de red utilizado, cada criterio (regla de acceso) ocupa una línea en la lista. En la figura 7-5 se muestra cómo funcionan las listas de acceso. Este ejemplo utiliza un enrutador que restringe el flujo de tráfico entre los diferentes departamentos de una organización.

A medida que cada paquete intenta ingresar a una interfaz, se examina su encabezado para ver si coincide con la lista de acceso. La tarea del enrutador es encontrar las coincidencias. Una vez que encuentra una, no se llevan a cabo evaluaciones adicionales. Si la regla que coincidió es de *permitir*, el paquete se envía a una interfaz de red en el otro lado del enrutador. Si la regla que coincidió es de *negar*, se elimina el paquete en la interfaz.

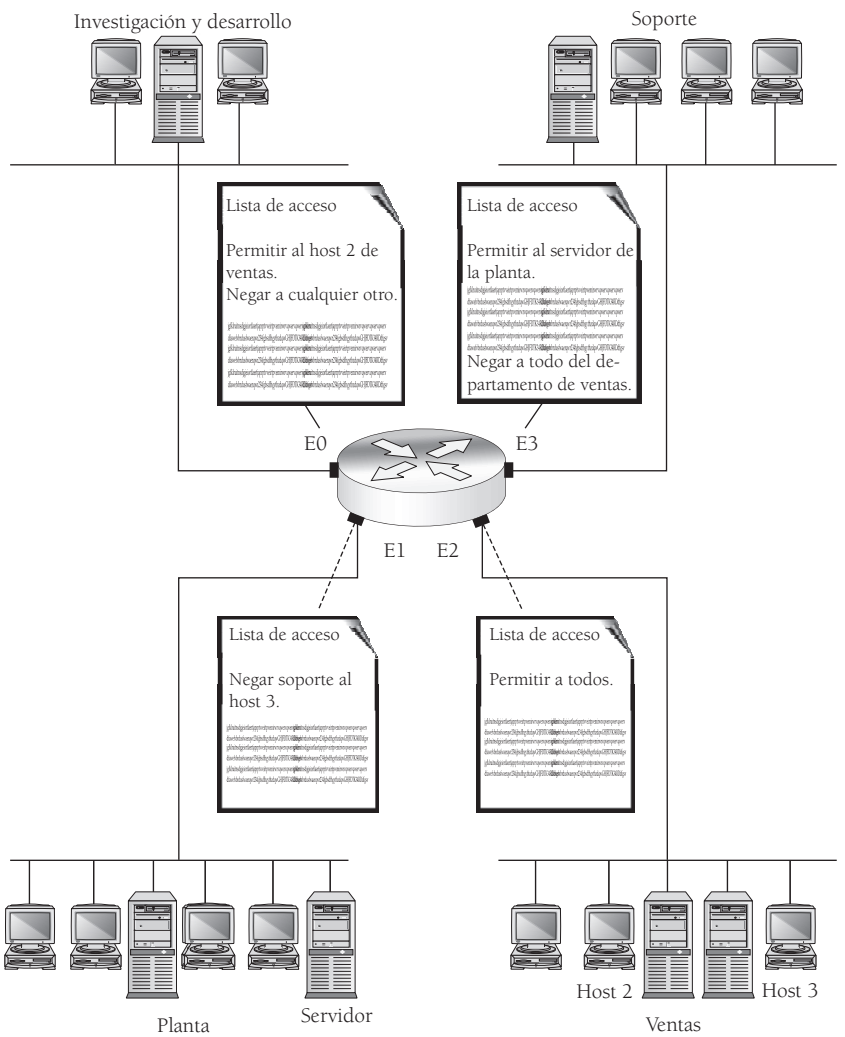


Figura 7-5. Una lista de acceso filtra los paquetes en cada interfaz del enrutador.

Si el proceso de evaluación de un paquete recorre toda la lista de acceso hasta el final sin que se haya encontrado una coincidencia, éste se elimina en forma predeterminada. A este mecanismo se le llama *regla de la negación implícita*, misma que proporciona una medida adicional de seguridad al administrar las condiciones no previstas en la lista de acceso.

El enrutador evalúa el paquete regla por regla, desde la línea del comienzo hasta el final. En la parte inferior de la figura 7-6 se ve un ejemplo tomado de una lista de acceso de un enrutador.

Comando	Nombre de la lista de acceso	Regla	Protocolo de transporte	Desde la dirección	Hacia la dirección		Protocolo de aplicación
Access-list	MiLista	permit	tcp	209.98.208.25	any	eq	http
		o deny	UDP ICMP	Podría ser cualquiera	Podría ser una dirección IP	Igual a	

Se necesita al menos una regla de autorización del protocolo de red para que la interfaz procese los paquetes.

Observe que las reglas que más coinciden se encuentran en la parte superior.

```
permit tcp any host 209.98.208.33 established (365135 matches)
permit udp host 209.98.98.98 host 209.98.208.33 (10322 matches)
permit tcp any host 209.98.208.33 eq smtp (888 matches)
permit tcp any host 209.98.208.33 eq pop3 (1126 matches)
permit tcp any host 209.98.208.33 eq 143 (2 matches)
permit tcp any host 209.98.208.33 eq telnet (2 matches)
permit icmp any 209.98.208.32.0.0.0.15 echo-reply
permit tcp host 134.84.244.7 209.98.208.0 0.0.0.115 eq telnet
```

Un protocolo de transporte tendrá todas las reglas necesarias para controlar los protocolos de aplicación.

"host" significa que no se permiten subredes, sino sólo los nodos de dirección IP del host.

"Desde" IP — "Hacia" IP — "Hacia" la máscara

Figura 7-6. Las instrucciones de las listas de acceso son reglas de seguridad.

Cada una de las líneas en la lista es una regla que autoriza o niega un tipo de tráfico específico. En la parte superior en la figura 7-6 se muestran las partes de un enunciado de la regla, iniciando con el comando **access-list** seguido de varios modificadores. Tenga presente que este ejemplo es para IP; la sintaxis varía ligeramente en el caso de los protocolos de red IPX, AppleTalk y otros que no son IP.

Una lista se acceso coherente se crea utilizando un nombre de lista de acceso común al comienzo de cada enunciado para una lista de acceso IP. Cada instrucción debe declarar un protocolo de transporte, como el Transmission Control Protocol (TCP, protocolo de control de transmisión), el User Datagram Protocol (UDP, protocolo de datagrama de usuario) o el Internet Control Messaging Protocol (ICMP, protocolo de mensajería de control de Internet). Si la regla implica una aplicación de red, la instrucción debe declarar primero un protocolo de transporte y terminar con el protocolo de aplicación. En la regla del ejemplo de la parte superior de la figura 7-6, el protocolo de transporte es TCP y el de aplicación es HTTP.

Tenga presente que las ACL también pueden tener otros protocolos:

- **ahp** Authentication Header Protocol (protocolo para la autentificación del encabezado).
- **eigrp** El Enhace Interior Gateway Routing Protocol (EIGRP, protocolo de mejora de enrutamiento de gateway interior), de Cisco.
- **esp** Encapsulation Security Payload (carga de seguridad de encapsulado).

- **gre** Túnel para el Generic Routing Encapsulation (GRE, encapsulado del enrutamiento genérico) de Cisco.
- **icmp** Protocolo de mensajería de control de Internet.
- **igmp** Internet Gateway Message Protocol (protocolo de mensajes para gateway de Internet).
- **ip** Cualquier protocolo de Internet.
- **ipinip** IP en túnel IP.
- **nos** Túnel IP sobre IP compatible con NOS KA9Q.
- **ospf** Protocolo de enrutamiento Open Shortest Path First (OSPF, abrir primero ruta más corta).
- **pcp** Protocolo para la Compresión de la Carga.
- **pim** Protocol Independent Multicast (transmisión múltiple independiente del protocolo).
- **tcp** Protocolo de Control para la Transmisión.
- **udp** Protocolo de Datagrama de Usuario.

Para aplicar una regla al tráfico entrante, debe poner la dirección IP externa del host en la posición *desde*, que siempre precede a la posición *hacia*. Este orden está invertido para restringir el tráfico saliente. El modificador **any** se utiliza para indicar todas las redes. Entonces, el enunciado en la parte superior de la figura 7-6 está indicando "Permita que el host 209.98.208.25 acceda a cualquier red para operar la aplicación HTTP sobre TCP".

La lista de acceso se activa en una interfaz utilizando el comando **access-group**, como se muestra en la siguiente secuencia de código. La primera línea "apunta" al IOS a la interfaz serial0, y la segunda línea aplica la lista de acceso 100 a todo el tráfico entrante que trata de ingresar a través del serial0:

```
MyRouter(config)#interface serial0
MyRouter(config-if)#ip access-group 100 in
```

Los enrutadores buscan coincidencias entre el contenido del encabezado del paquete y la lista de acceso de la interfaz. Una coincidencia sería una dirección origen o de destino, un protocolo o un número de puerto. Si la regla de coincidencia es una regla de aceptación, se envía el paquete. Sin embargo, si la regla de coincidencia es una regla de negación, se elimina el paquete sin hacer alguna evaluación sobre cualquier regla que haya en adelante en la lista.

Una lista de acceso puede tener todas reglas de filtrado que se desee; el límite práctico es la cantidad de memoria del enrutador que desee utilizar para el filtrado de seguridad y no para el enrutamiento productivo. Debido a que las reglas de la lista de acceso se evalúan de arriba abajo, las coincidencias más frecuentes deben colocarse en la parte superior de la lista, para no desperdiciar ciclos de procesamiento en la CPU del enrutador.

Tenga presente que una lista de acceso por sí sola no convierte un enrutador en firewall. Casi todas las listas de acceso se utilizan para la administración básica del tráfico en las interconexiones. Sin embargo, podría configurar físicamente un enrutador como punto de ahogamiento, de tal forma que todo el tráfico pase por una lista de acceso, lo que lo convertiría en un firewall ligero. Lo anterior se hace a menudo para restringir el acceso entre las redes que conforman una interconexión. En realidad, el estándar IOS tiene docenas de comandos orientados a la seguridad, aparte del comando **access-list** que también se utiliza en los productos firewall de Cisco. Sin embargo, depender de la lista de acceso como parte medular de la configuración de un firewall da como resultado una seguridad cuestionable.

Los firewalls rastrean las sesiones de interconexión

La tecnología del firewall se basa en las listas de acceso que rastrean las sesiones. A esta tecnología se le llama filtrado de paquetes *basado en el contexto* o *con estado*, porque un paquete individual puede manejarse con base en el contexto más grande de su conexión. Este tipo de filtrado utiliza lo que algunos llaman *listas de acceso reflejas*, porque su contenido cambia dinámicamente como respuesta refleja al estado de la sesión individual (si la sesión inicia desde un host interno, por cuánto tiempo ha estado operando, etcétera). En la figura 7-7 se muestra la manera en que los firewalls basados en el contexto rastrean las sesiones.

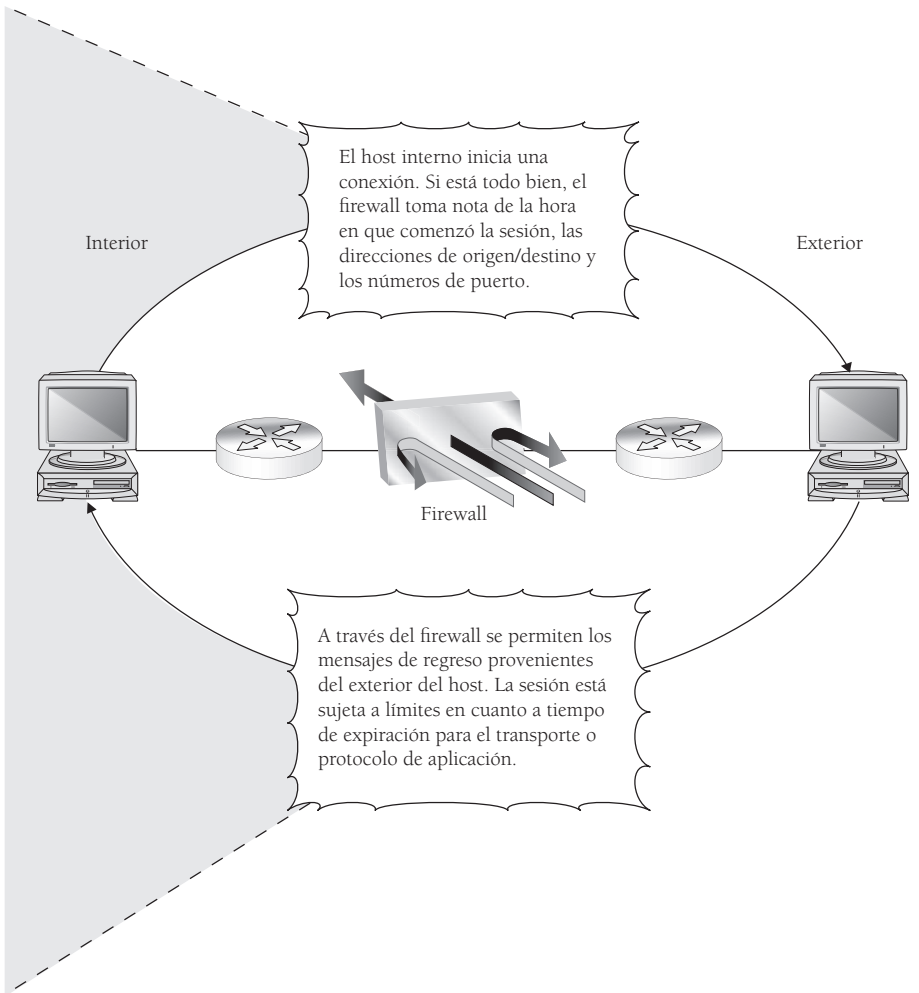


Figura 7-7. Los firewalls basados en el contexto rastrean los estados de la conexión.

NOTA TCP y UDP son protocolos que operan en el nivel del transporte (capa 4) del modelo de referencia OSI de siete capas. TCP son las siglas de Transmission Control Protocol (protocolo de control para la transmisión); es un protocolo orientado a la conexión diseñado para entregar comunicaciones full-duplex con entrega garantizada. Gran parte del tráfico IP pasa a través de conexiones TCP. UDP son las siglas de User Datagram Protocol (protocolo de datagrama de usuario), un protocolo sencillo no orientado a la conexión con baja información redundante, que no cuenta con entrega garantizada de corrección de errores. UDP se utiliza en aplicaciones relativamente simples como TFTP (Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos). Un tercer protocolo de transporte es ICMP (Internet Control Message Protocol, protocolo de mensajería de control de Internet), que es un protocolo especializado que se usa en aplicaciones como **ping** y **traceroute**. Los protocolos de transporte se estudiaron en el capítulo 2.

El lector astuto se podría preguntar cómo rastrea un firewall sesiones UDP, si éste es un protocolo de transporte no orientado a la conexión que carece de los protocolos de saludo formales y reconocimientos del TCP. El filtrado en el UDP trabaja tomando nota de la dirección origen/destino y el número de puerto de la sesión, y después haciendo una estimación de que todos los paquetes que compartan esas tres características pertenecen a la misma sesión. Debido a que los periodos de expiración son muy breves para las sesiones UDP (por lo general una fracción de los tiempos máximos establecidos para las sesiones TCP), la estimación del firewall casi siempre es correcta.

Utilización de las direcciones globales para esconder la topología interna de la red

El software IOS de Cisco tiene una capacidad llamada Network Address Translation (NAT, traducción de direcciones de red), utilizada por los enrutadores y firewalls para enmascarar las direcciones internas de red par del mundo exterior. Como se analizó en el capítulo 2, IP permite el uso de direcciones privadas en lugar de registradas (por ejemplo, 10.1.13.1 en lugar de 209.78.124.12). Lo anterior se hace por muchas razones: la principal es conservar direcciones (a veces llamada *espacio de direcciones*), porque simplemente no hay direcciones IP suficientes para numerar de manera única a todos los hosts, dispositivos y LAN de la mayor parte de las interconexiones. Se puede operar una interconexión sin direcciones privadas, pero esto se hace en muy raras ocasiones.

A medida que los paquetes se envían al exterior, la NAT sobrescribe la dirección interna de red en el campo de dirección de origen con una dirección IP completa. Esto se lleva a cabo desde un conjunto de direcciones IP registradas que se encuentra a disposición de la NAT, que las asigna entonces a las conexiones salientes a medida que éstas se reestablecen. La NAT compara la dirección local interna con la del conjunto, elimina la comparación cuando se termina la conexión y reutiliza la dirección del conjunto para la próxima conexión saliente que se presente. Como se observa en la parte superior de la figura 7-8, la traducción NAT se lleva a cabo de uno en uno. Por tanto, a pesar de que la NAT esconde direcciones internas, no conserva el espacio de direcciones.

En la parte inferior de la figura 7-8 se muestra que la NAT también puede configurarse para utilizar sólo direcciones registradas para todos los anfitriones internos que establezcan conexiones con el exterior. A esta función se le conoce con el nombre de Port Address Translation (PAT, traducción de las direcciones del puerto); a diferencia de la NAT, traduce a

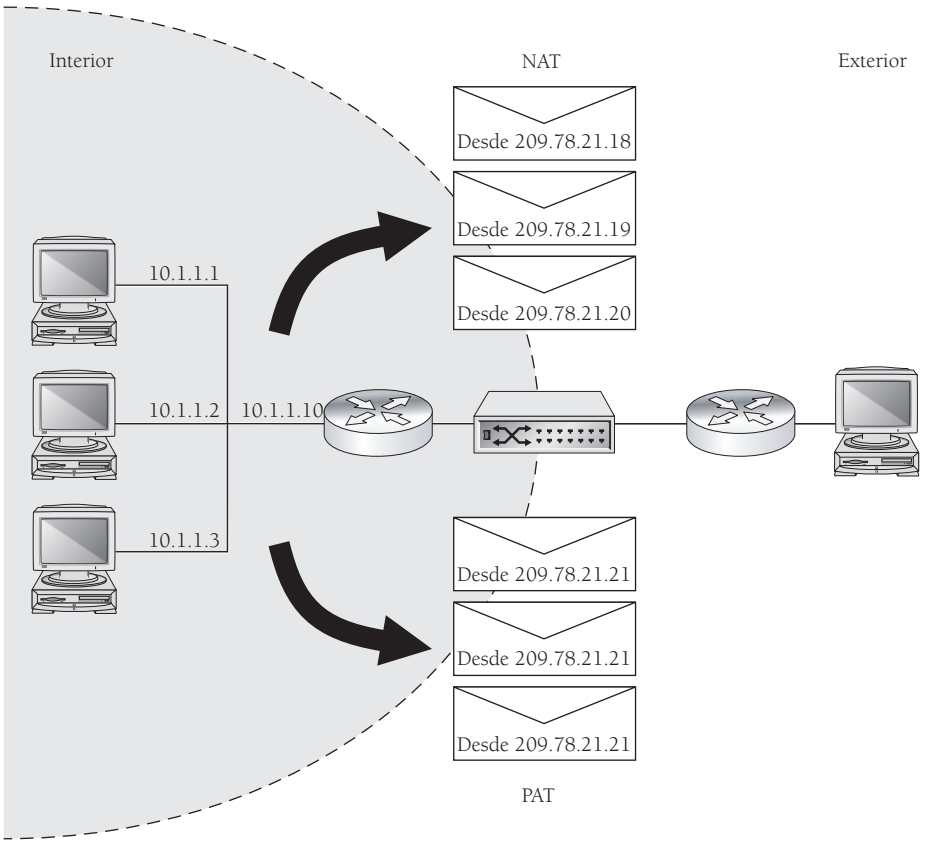


Figura 7-8. Las direcciones internas del host pueden traducirse una por una en una dirección global.

una dirección externa global en lugar de direcciones externas individuales. PAT proporciona seguridad adicional al imposibilitar a los hackers la identificación de los hosts individuales dentro de una interconexión privada, porque todos aparentan venir de la misma dirección host. Además de mejorar la seguridad, la PAT también conserva el espacio para direcciones.

La traducción de direcciones es un ejemplo del valor del rastreo de sesiones basada en el contexto. Sin la capacidad de rastrear la sesión a la que pertenece un determinado paquete, no sería posible la asignación dinámica y la comparación de las direcciones internas con las públicas.

Servidores proxy

Un *servidor proxy* es una aplicación que actúa como intermediaria entre dos sistemas terminales. Los servidores proxy trabajan en la capa de la aplicación (capa 7) del firewall, donde se fuerza a que ambos extremos de una conexión conduzcan la sesión mediante el proxy. Para ello, generan y operan un proceso en el firewall que imita un servicio como si estuviera

operando en el host terminal. Como se muestra en la figura 7-9, un servidor proxy convierte, en esencia, una sesión de dos entidades en una de cuatro; en ella, los dos procesos intermedios emulan a los dos hosts reales. Como trabajan en la capa 7, a los servidores proxy también se les conoce como *firewalls de la capa de la aplicación.*

Debe operarse un servicio proxy para cada tipo de aplicación de Internet que habrá de soportar el firewall: un proxy de Simple Mail Transport Protocol (SMTP, protocolo simple de transporte de correo) para el correo electrónico, un proxy HTTP para los servicios de Web, etcétera. En un sentido, los servidores proxy son arreglos de una sola vía que funcionan de un lado de la red a otro. En otras palabras, si un usuario interno desea acceder a un sitio Web en Internet, los paquetes que conforman esa solicitud se procesan mediante el servidor HTTP antes de ser enviados al sitio Web. Los paquetes que regresan del sitio Web son, a su vez, procesados mediante el servidor HTTP antes de enviarse de regreso al host interno del usuario. Al igual que con la NAT, los paquetes circulan hacia el servidor Web externo transportando la dirección IP del servidor HTTP en lugar de la dirección interna del host. En la figura 7-9 se describe un firewall en que están operando varios servidores proxy a la vez.

Debido a que los servidores proxy centralizan toda la actividad de una aplicación en un solo servidor, éstos presentan la oportunidad ideal para llevar a cabo gran variedad de funciones útiles. El hecho de que la aplicación opere en el firewall representa una oportunidad para inspeccionar no sólo las direcciones de origen, destino y número de puerto de los paquetes, sino muchas cosas más. Por ello, casi todos los firewalls modernos incorporan alguna forma de arquitectura proxy-servidor. Por ejemplo, pueden inspeccionarse los

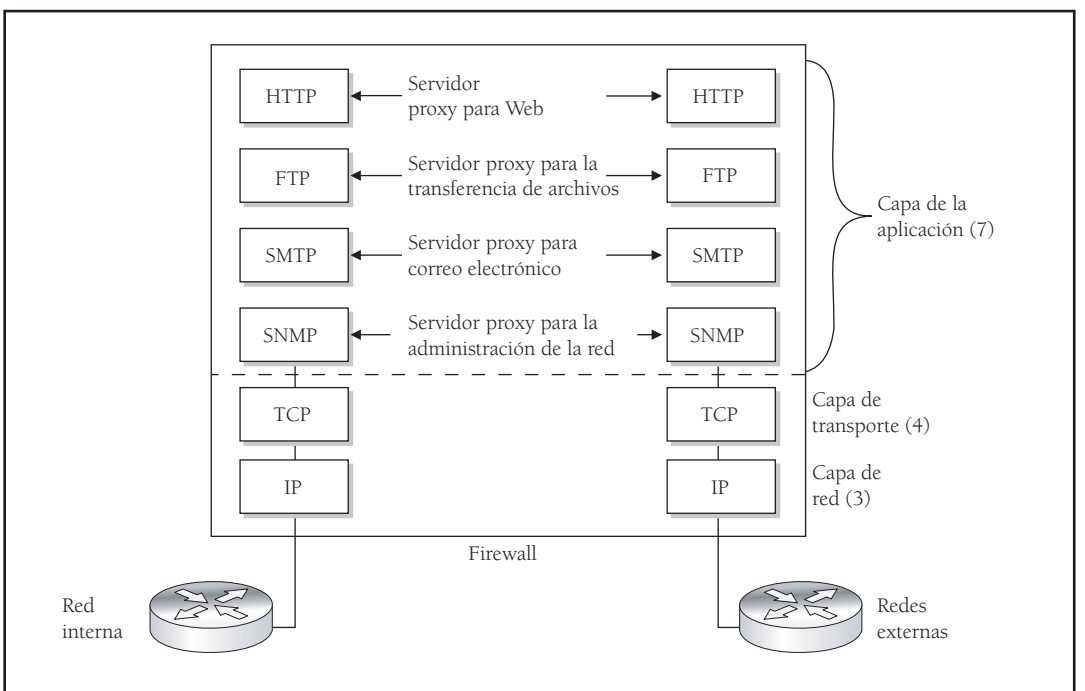


Figura 7-9. La tecnología del servidor proxy es la base de los firewalls avanzados.

paquetes entrantes dirigidos a un servidor configurado exclusivamente para proporcionar información (digamos, un servidor FTP) para ver si éste contiene algunos comandos escritos (como **PUT**). De esta forma, el servidor proxy sólo permitiría conexiones que contengan comandos de lectura.

El servidor proxy es otra tecnología posible sólo en el contexto de los firewalls. Por ejemplo, si un firewall soporta miles de conexiones simultáneas debe, por supuesto, decidir a qué sesión pertenece cada uno de los millones de paquetes entrantes con el número de puerto 80 (HTTP).

Configuraciones de doble base

Una configuración firewall de *doble base* suele implementarse con la capacidad de enrutar tráfico apagado entre las tarjetas de interfaz de red, sin inspeccionarlo. Una configuración de doble base obliga a que todo el tráfico circule por un servicio proxy antes de que pueda enrutarse a otra interfaz; por ello, los firewalls de servidor proxy utilizan configuraciones de doble base, como se muestra a la izquierda de la figura 7-10. Otro de los usos de la doble base es cuando desea que los usuarios de dos redes (digamos, los departamentos de investigación y desarrollo y de ventas) accedan a un solo recurso pero sin que se enrute tráfico entre ellos. Entonces se deshabilitaría cualquier capacidad de enrutamiento entre las dos interfaces. La configuración que se encuentra a la derecha de la figura 7-10 muestra lo anterior.

Si se utiliza una configuración de doble base en esta forma no se genera una compuerta firewall en sí, porque el tráfico entrante no está dirigido más allá del servidor. Sólo se trata de una manera fácil de hacer que un servidor se haga cargo de dos departamentos que no debn intercambiar tráfico. Además, es una forma de asegurarse de que el tráfico no se intercambie, porque los servicios de enrutamiento están deshabilitados dentro del enrutador.

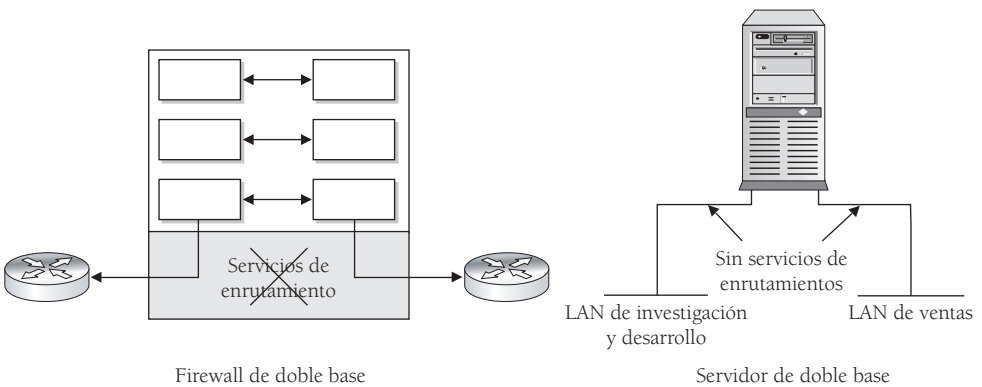


Figura 7-10. Las configuraciones de doble base apagan los servicios de enrutamiento dentro del dispositivo.

Registro y notificación de eventos

La conservación de registros es una parte importante del papel de un firewall. Cuando el firewall niega el acceso a un paquete, el evento se registra en un archivo llamado *syslog* (abreviatura en la industria de system record, registro del sistema) o en un sistema de registro propiedad del fabricante del firewall. Casi todos los firewalls pueden configurarse para subir información de registro a un servidor de registro en otra parte de la red, donde puede ser analizado para ver si cumple con las directivas de seguridad de la compañía.

También es posible configurar los firewalls para que generen mensajes de alerta, si se sobrepasan los límites especificados. En algunas operaciones de red más sofisticadas, dichas alertas se envían directamente a una consola atendida, de manera que el equipo encargado de la administración de la red pueda responder al evento tomando una de varias medidas (por lo general, apagando la interfaz de red donde se está presentando la violación a la seguridad).

El conjunto de características del firewall del IOS

El firewall del IOS es una opción de valor agregado al software IOS de Cisco. Se consigue como un *grupo de características* del IOS (los grupos de características se estudian en el capítulo 4). El firewall del IOS se utiliza para convertir un enrutador Cisco estándar en un firewall muy robusto, agregando varias funciones de seguridad sobre el filtrado básico de tráfico del software IOS estándar:

- **Context-Based Access Control (CBAC, control de acceso basado en el contexto)** Es una forma avanzada de filtrado de tráfico que analiza la información de la capa de la aplicación (capa 7), como el HTTP, para aprender acerca del estado de las conexiones TCP y UDP.
- **Traducción de direcciones (PAT y NAT)** Oculta las direcciones IP internas insertando direcciones de origen ocultas en los paquetes que se envían fuera del firewall. PAT y NAT ocultan a los hackers la topología de la red interna.
- **Soporte del servidor de seguridad** El enrutador puede configurarse como cliente de los servidores de seguridad TACACS+, RADIUS o Kerberos, en que los nombres de usuario y contraseñas pueden almacenarse en la base de datos de autentificación del usuario del servidor.
- **Detección de ataque de Negación del Servicio** Detecta los patrones de tráfico característicos de los ataques de *Denial-of-Service (DoS, negación del servicio)* y envía mensajes de alerta (estos ataques intentan negar el servicio saturando una red con solicitudes de servicio, como comandos ilegales de correo electrónico o un gran número de correos electrónicos).
- **Network-Based Application Recognition (NBAR, reconocimiento de la aplicación basada en la red)** Reconoce muchas aplicaciones diferentes y puede utilizar servicios especiales con base en ellos.
- **Bloqueo de Java** La capacidad de bloquear mensajes de Java selectivamente (los applets de Java son programas descargables que operan por su cuenta y que pueden programarse para provocar daño a cualquier sistema host que tenga la mala fortuna de ejecutarlos).
- **Cifrado** La capacidad de hacer incomprensible el contenido de un paquete a todos los sistemas, con excepción de los que cuentan con una clave para decodificarlos.

- **Autentificación del enrutador vecino** Comando que permite al enrutador obligar a un enrutador vecino a autentificar su identidad o bloquear todos los paquetes enviados desde él.
- **Alertas de seguridad y registro de eventos** Son mensajes que alertan a la administración de la red de un problema de seguridad y el registro de todos los eventos de seguridad para su posterior recopilación y análisis.
- **Soporte de VPN y QoS** Proporciona el túnel y las características de QoS (Quality of Service, calidad de servicio) para asegurar las VPN. Esta característica brinda túneles codificados en el enrutador, a la vez que garantiza seguridad robusta, validación del nivel del servicio, detección de intrusiones y administración avanzada de ancho de banda.
- **Práctica de auditoría** Permite varias características para el rastreo detallado. Registra hora, host de origen, host de destino, puertos, duración y número total de bytes transmitidos, para el reporte detallado. Se configura con base en las aplicaciones y características.
- **Comparación de puertos dinámicos** Permite que las aplicaciones basadas en el CBAC sean operadas en puertos no estándares. Esto hace posible que los administradores de red puedan diseñar a su voluntad el control de acceso de determinadas aplicaciones y servicios.
- **Administración del firewall** Los firewalls se configuran con una interfaz amigable de usuario que proporciona ayuda paso a paso en diseño de la red, su direccionamiento y la configuración de la directiva de seguridad del firewall del IOS.
- **Integración con el software IOS de Cisco** Este conjunto de características interactúa con las del IOS de Cisco, integrándolas en la directiva de seguridad.
- **Soporte de interfaz múltiple basada en directiva** El acceso al usuario puede controlarse con base en la dirección IP y la interfaz. El acceso está determinado por la directiva de seguridad.
- **Redundancia/falla** Enruta tráfico automáticamente a un enrutador secundario en caso de una falla.
- **Listas de acceso con base en el tiempo** La directiva de seguridad puede establecerse con base en la hora del día y en el día de la semana.
- **Sistema de prevención de intrusiones** Sistema de detección en línea que responde a la actividad sospechosa. El enrutador puede configurarse para registrar el evento, enviar un mensaje al administrador del sistema o negar el acceso a la dirección IP del intruso.
- ▲ **Proxy de autentificación** Las directivas de seguridad pueden establecerse usuario por usuario.

Cómo funciona el control de acceso basado en el contexto

El control de acceso basado en el contexto es un conjunto de comandos del IOS para inspeccionar paquetes de manera mucho más cercana que las listas de acceso normal. El CBAC funciona rastreando las conexiones externas iniciadas en el interior del firewall. El CBAC identifica sesiones rastreando las direcciones IP de origen/destino y los números de puerto origen/destino extraídos de los paquetes. Cuando regresa una respuesta del host remoto de la sesión en la forma de tráfico entrante, el CBAC determina la sesión a la que pertenecen los paquetes de

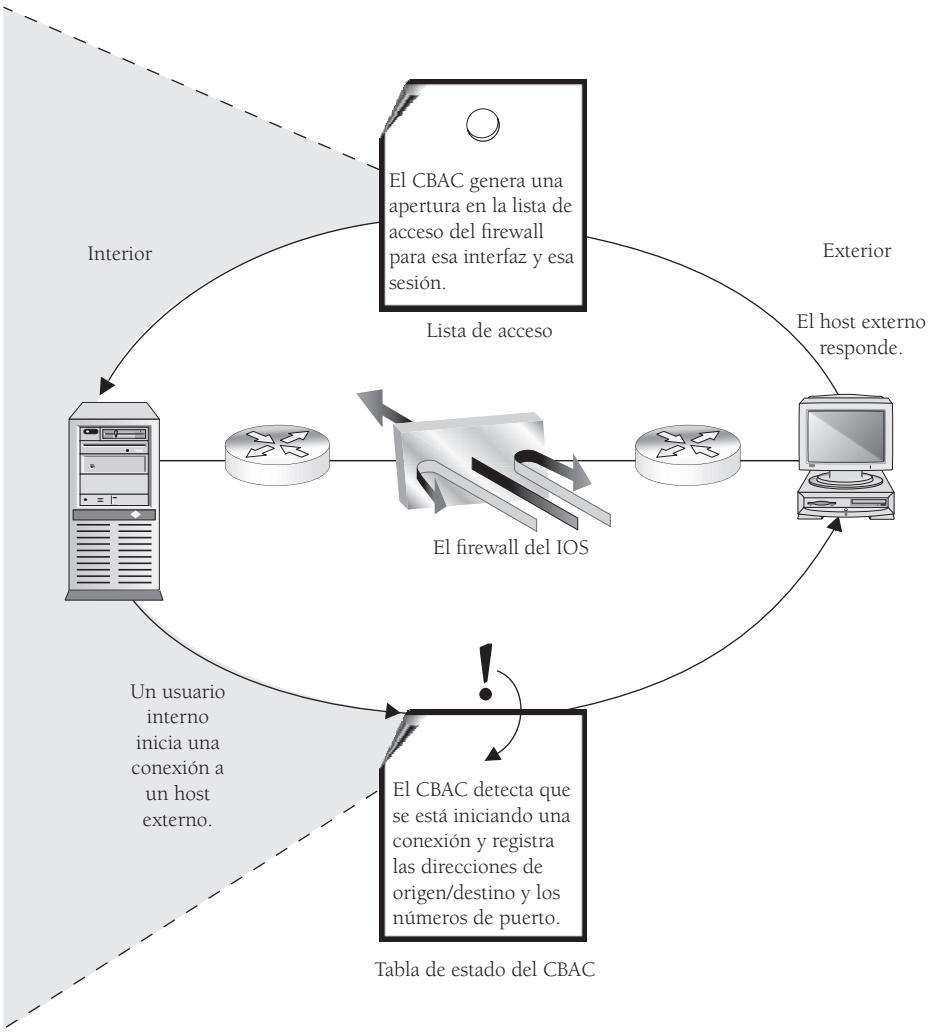


Figura 7-11. El CBAC crea aperturas temporales con base en el estado de la conexión.

entrada. De esta forma, el CBAC conserva una lista dinámica de las sesiones en progreso y puede hacer malabares con las excepciones de seguridad de un momento a otro. Esta lista dinámica, llamada *tabla de estado*, rastrea el estado de sesiones válidas hasta el momento en que éstas terminan. La tabla de estado del CBAC se mantiene por sí sola eliminando sesiones cuando los usuarios las terminen o después de un periodo máximo permitido de inactividad llamado *tiempo máximo de espera*. El administrador de red especifica los valores de éste para cada uno de los protocolos de transporte. En la figura 7-11 se muestra el proceso CBAC.

El CBAC utiliza la tabla de estado para realizar ingresos y eliminaciones dinámicas a la lista de acceso de la interfaz. Momentáneamente, se permiten la dirección origen/destino o los números de puerto que suelen bloquearse con la lista de acceso, pero sólo para una sesión que el CBAC sepa que sea válida y que se haya iniciado desde el perímetro de seguridad del firewall. El CBAC genera aperturas en el firewall conforme se necesiten para permitir el tráfico de regreso. Una vez que termina la sesión, la prohibición de la lista de acceso se aplica de nuevo hasta que otra sesión llame desde la tabla de estado del CBAC, preguntando por una excepción temporal propia.

Si, al parecer, el enrutador está saturado por tanta complejidad, recuerde que las tablas de estado y las listas de acceso se administran interfaz por interfaz. Cada interfaz de un enrutador Cisco que opere el firewall del IOS cuenta con su propia lista de acceso, sus reglas de inspección y sus sesiones válidas. Una buena configuración de firewall puede reducir gran parte de la complejidad que debe enfrentar agrupando tipos o fuentes similares de tráfico en interfaces de red específicas.

Funciones principales del firewall del IOS

El firewall del IOS obliga selectivamente a que se cumplan las reglas de seguridad con base en el contexto de cada sesión. Para conseguir esto en forma completa, el firewall del IOS debe inspeccionar los paquetes mucho más de cerca que como lo hacen las simples listas de acceso. Por ello, el software del firewall del IOS es específico en la aplicación de las reglas de inspección. La palabra *específico* significa aquí que las reglas de inspección se aplican de manera mucho más selectiva que el esquema permitir/negar "todo o nada" que usan las listas de acceso. Esto hace que el firewall sea más flexible y que represente una barrera de seguridad más difícil de vencer. No profundizaremos mucho en las características de inspección del firewall del IOS, porque se trata de un libro para principiantes, pero un repaso rápido ilustrará la manera en que la tecnología del firewall funciona en la inspección de paquetes:

- **Inspección SMTP** Gran parte de los peores ataques de virus penetran en las interconexiones seguras por medio del correo electrónico. En lugar de verificar únicamente el número de puerto SMTP de cada paquete, el firewall del IOS verifica que los paquetes SMTP no tengan comandos ilegales. Cualquier paquete SMTP que contenga un comando diferente a los 12 legales, se eliminarán por considerarse subversivos.
- **Inspección de Java** Algunas directivas de seguridad de red prohíben la descarga de applets de Java desde el exterior de las redes, debido a su poder de destrucción. No puede establecerse una directiva de seguridad que obligue a todos los usuarios internos a deshabilitar Java en sus navegadores Web. El firewall del IOS le permite bloquear applets de Java entrantes y también designar una lista de sitios externos de confianza (amigables), que no tendrá bloqueada la descarga de applets de Java (o podría permitir los applets desde todos los sitios, con excepción de los definidos explícitamente como hostiles).
- **Inspección H.323** NetMeeting es una aplicación importante del protocolo H.323 que requiere el uso de un segundo canal (sesión) además del canal H.323 que se mantiene en la tabla de estado de CBAC. Puede configurarse el firewall del IOS para verificar un canal TCP genérico, además del canal H.323, para permitir que las conexiones NetMeeting funcionen a través del firewall.

- **Inspección del RPC** El comando de inspección RPC (Remote Procedure Call, llamada a procedimiento remoto) del firewall del IOS acepta la entrada de números de programa. Por ejemplo, si el número de programa para NFS (Network File System Protocol, protocolo del sistema de archivos de red) se especifica en un comando RPC, entonces el tráfico NFS puede operar a través de esa interfaz del firewall.

Configuración del firewall del IOS

La traducción de direcciones se configura en el firewall del IOS utilizando los comandos **nat** y **pat**. Por lo general, el primer paso de la configuración del firewall del IOS es configurar las traducciones de tal forma que enmascaren las direcciones IP internas del mundo exterior. Algunas configuraciones de ejemplo de NAT y PAT se proporcionan en la próxima sección de este capítulo, que estudia el firewall PIX.

La seguridad basada en el contexto se configura en el firewall del IOS creando reglas de inspección. Éstas (también llamadas *grupos de reglas*) se aplican a las listas de acceso que rigen a interfaces específicas de red del firewall. Entonces, la configuración del firewall del IOS se lleva a cabo, sobre todo, utilizando dos variaciones de dos comandos:

- **access-list** Es un comando utilizado para definir las reglas básicas de acceso a la interfaz.
- **ip inspect** Es un comando utilizado para definir qué CBAC se buscará en la interfaz.

La lista de acceso especifica cuáles reglas normales se aplican al tráfico que ingresa a la interfaz y se utiliza para indicarle a la interfaz las aplicaciones de red (números de puerto) que están prohibidos, las direcciones de destino que se encuentran bloqueadas, etcétera. Las reglas de inspección del CBAC modifican dinámicamente la lista de acceso conforme sea necesario para crear aperturas temporales en el firewall del IOS para sesiones válidas. El CBAC define una sesión válida como cualquier conexión TCP o UDP que coincida su criterio en la lista de acceso.

Además de crear aperturas temporales en el firewall, el CBAC aplica las reglas de inspección para detectar varios tipos de ataques de red y generar mensajes de alerta, que suelen enviarse a la consola de administración de la red.

NOTA Uno de los ataques de negación del servicio más conocidos es SYNflood, así que recibe su nombre por el bit SYB que inicia un saludo de tres vías que se utiliza para configurar las conexiones TCP. Los ataques del SYNflood intentan saturar la red de destino en una inundación de intentos de conexión (y, por tanto, negando a los hosts legítimos el servicio de red). El administrador de la red utiliza un comando llamado **ip inspect tcp synwait-time** para indicarle al firewall del IOS por cuánto tiempo se retendrá un bit SYN no respondido antes de eliminarlo. Al no permitir que los bits SYN se acumulen, el comando **ip inspect tcp synwait-time** puede utilizarse para frustrar este tipo de ataque de negación de servicio.

Es posible configurar el firewall del IOS de dos formas, si la configuración del firewall incluye una DMZ. En la figura 7-12 se muestra lo anterior. La configuración que se encuentra a la derecha de la figura 7-12 muestra la lista de acceso extraída del firewall.

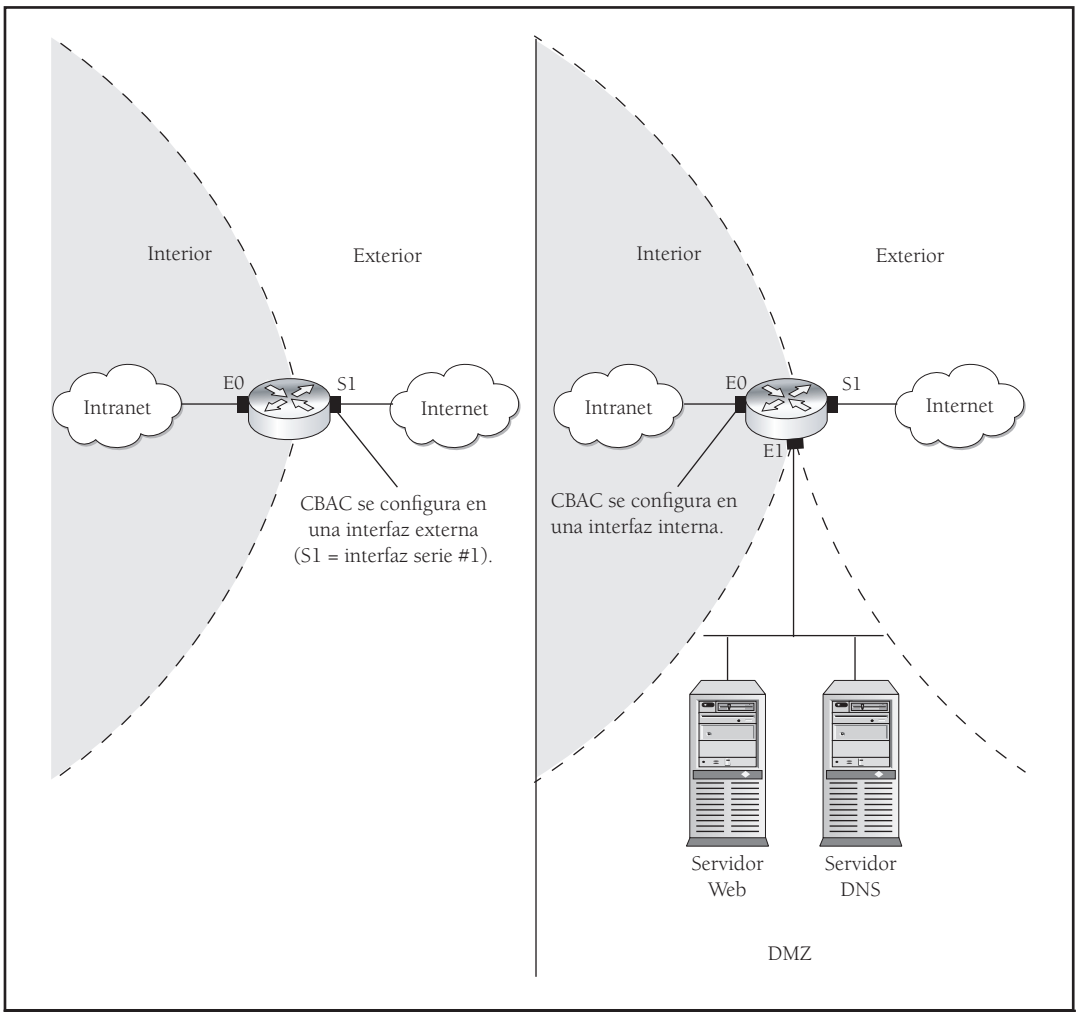


Figura 7-12. CBAC puede configurarse en la interfaz interna o externa.

Si se configura el CBAC en la interfaz interna, se libera al firewall de la tarea de crear y eliminar excepciones a la regla con base en el contexto para el tráfico que llega al servidor Web (HTTP) y al servidor DNS (Domain Name System, sistema de nombres de dominio) de la DMZ. Con este arreglo, el CBAC aún puede controlar selectivamente el acceso de los usuarios internos a los servicios HTTP y DNS, pero no se tendrá que preocupar de las conexiones que llegan a los servidores DMZ.

NOTA El firewall del IOS es una versión del software IOS de Cisco; por ello, se aplican las convenciones normales del IOS. Para configurar el firewall del IOS, primero debe acceder a un enrutador a través de Telnet, SSH o la interfaz del navegador del Web; ingrese en modo de comando Privileged Exec; y después ingrese el modo de configuración, con

la solicitud firewall(config-if)# apuntando a la interfaz a la que se aplicará la configuración CBAC.

El primer paso en la configuración de la interfaz firewall del IOS es crear una lista de acceso. Para definirla, utilice la sintaxis de comando siguiente:

```
Firewall(config)#ip access-list standard access-list-name-or-number
Firewall(config-std-nacl)#permit ....
```

Si una regla de permiso coincide, el paquete se envía a través del firewall. Las reglas de negación se definen utilizando la misma sintaxis:

```
Firewall(config)#ip access-list standard access-list-name-or-number
Firewall(config-std-nacl)#deny ....
```

Si una regla de negación coincide, el paquete se elimina. En la figura 7-13 se muestra un ejemplo de lista de acceso 100. Esta lista se aplicará a la interfaz firewall de Ethernet0. La lista de acceso 100 permite todo el tráfico que deba ser inspeccionado por el CBAC. La última línea de la lista de acceso está configurada para negar los protocolos IP desconocidos que un intruso podría tratar de utilizar.

El segundo paso en la configuración del CBAC es definir un conjunto de reglas de inspección con el comando **ip inspect name**, utilizando la sintaxis siguiente:

```
Firewall(config)#ip inspect name inspection-name protocol [timeout
seconds]
```

La sintaxis de este comando indica al firewall del IOS para qué se verificarán los paquetes y el máximo periodo de inactividad que se permitirá antes de cerrar cualquier sesión creada con la regla de inspección. Los periodos de expiración son importantes en las configuraciones del CBAC. Si los límites de tiempo máximo de espera son muy altos, la tabla de estado podría saturarse, lo que afectaría el desempeño del enrutador y aun la seguridad. Por otro lado, si los periodos de expiración son muy bajos, los usuarios podrían frustrarse porque tendrían que restablecer con mucha frecuencia las conexiones hechas a los hosts de Internet.

Un conjunto de reglas de inspección se crea utilizando el mismo *inspection-name* en todos los comandos que se incluirán en el grupo. El siguiente fragmento de código muestra un grupo de reglas de inspección que se está construyendo bajo el nombre Rulz. Al compartir el nombre Rulz, es posible invocar con una sola instrucción los ocho comandos **ip inspect**

SMTP está bien si se encuentra dirigido a un host de administración.

```
access-list 100 permit tcp any 179.12.244.1 eq smtp
access-list 100 permit tcp 209.43.23.201 any eq 80
```

Un host interno es adecuado para HTTP.

Figura 7-13. Esta lista de acceso establece el tráfico en Ethernet0 para la inspección CABC.

Protocolos de la capa de transporte	Palabra clave
TCP, protocolo de control para la transmisión	Tcp
UDP, protocolo de datagrama de usuario	Udp
ICMP, protocolo de mensajería de control de Internet	
Protocolos de la capa de la aplicación	
Firewall de aplicación	**appfw**
CU-SeeMe	**cuseeme**
ESMTP	**smtp**
FTP	**ftp**
IMAP	**imap**
Java	**http**
H.323	**h323**
NetShow de Microsoft	**netshow**
POP3	**pop3**
RealAudio	**realaudio**
RPC	**rpc**
SIP	sip
SMTP, protocolo de transferencia de correo simple	**smtp**
Skinny Client Control Protocol (SCCP, protocolo delgado para el control del cliente)	**skinny**
Structured Query Language*Net (SQL*Net, lenguaje estructurado para consultas*Net)	**sqlnet**
TFTP	**tftp**
Comandos UNIX R (rlogin, rexec, rsh)	**rcmd**
VDOLive	**vdolive**
WORD	**Nombre de aplicación definida por el usuario, usar prefijo de usuario**

Tabla 7-1. Palabras clave de los comandos ip Inspect y Access-List del firewall del IOS.

name incluidos en este grupo. En la tabla 7-1 se proporcionan las palabras clave utilizadas por los comandos de inspección de protocolos.

```
Firewall(config)#ip inspect name Rulz ftp timeout 2000
Firewall(config)#ip inspect name Rulz smtp timeout 3000
Firewall(config)#ip inspect name Rulz tftp timeout 60
```

```
Firewall(config)#ip inspect name Rulz http java-list 99 timeout 3000
Firewall(config)#ip inspect name Rulz udp timeout 15
Firewall(config)#ip inspect name Rulz tcp timeout 2000
```

Los límites de tiempo máximo de espera en el ejemplo anterior permiten que las aplicaciones TCP respondan en tres o cinco minutos, aproximadamente, y las aplicaciones UDP en un minuto o menos. Esto refleja el hecho de que las aplicaciones UDP están más preocupadas por causar un mínimo de información redundante en la red que por la integridad de la sesión. Los tiempos de expiración fijados para el TCP y el UDP son anulados en sesiones que operan un protocolo de aplicación. Por ejemplo, cualquier sesión de copia de seguridad TFTP que opere en este firewall tendría el límite de 60 segundos de tiempo máximo de espera fijado para TFTP (previniendo el límite de 15 segundos fijado para sesiones de UDP solamente).

Aunque es verdad que los tiempos máximos de espera ayudan a conservar los recursos del sistema, la razón principal para configurarlos en un firewall es la seguridad. Cuanto menos tiempo dé a un programa de ataque de un hacker para que trate de llegar a la interfaz del firewall, mejor será la seguridad de su interconexión. Sin embargo, los tiempos máximos de espera no pueden establecerse con una tolerancia muy estricta; de otra forma, los usuarios legítimos tendrán que hacer muchos intentos para conectarse. Como todo lo demás en el ámbito de la conectividad, la estrategia de los tiempos máximos de espera es cuestión de equilibrio.

Aunque el grupo de inspección y la ACL no tienen nada que ver entre sí, ambos se aplican a la interfaz. De modo que el último paso en la configuración de una interfaz firewall del IOS es aplicar un grupo de reglas de inspección a la lista de acceso. El CRAC modificará entonces la ACL de acuerdo con el grupo de inspección. El fragmento siguiente, tomado del archivo config para la interfaz del firewall Ethernet0, muestra el grupo de inspección Rulz y la lista de acceso 89. Las reglas se han aplicado a la inspección y filtrado del tráfico entrante.

```
interface Ethernet0
  description Velte Extranet Gateway
  ip address 209.78.124.12 255.255.255.248
  ip broadcast address 209.78.124.1
  ip inspect Rulz in
  ip access-group 89 in
```

Sin reglas de inspección que modifiquen las listas de acceso, el comportamiento del firewall del IOS regresará al de un enrutador normal que opera listas de acceso normales.

Características de la administración de sesiones del firewall del IOS

Por el momento, ha visto la importancia que tiene el tiempo para los firewalls. Esto no es diferente a la función del jefe de seguridad de un banco de mantener estricto control sobre el tiempo que permanece abierta la puerta de seguridad cuando la gente ingresa o sale del banco. Por razones obvias, el jefe de seguridad hará un gesto de enojo a los empleados que estén merodeando por la puerta de seguridad.

Los comandos de sesión max-incomplete De la misma forma que el jefe de seguridad de un banco, los administradores de red se ponen nerviosos con las conexiones pendientes

en las interfaces del firewall, sobre todo en las interfaces externas. A estas conexiones incompletas se les llama *sesiones medio abiertas*. Un número cada vez mayor de sesiones medio abiertas en el firewall podrían indicar que se está gestando un ataque de negación de servicio. El firewall del IOS cuenta con varios comandos, llamados comandos de intercepción TCP, que interceptan los ataques DoS antes de que puedan saturar la interfaz de red del firewall.

El firewall del IOS utiliza el comando **ip inspect max-incomplete** para rastrear y controlar sesiones medio abiertas. Para TCP, *medio abierto* significa que una sesión aún no ha alcanzado el estado establecido (de hecho, ingresa a la tabla de estado del CBAC como una solicitud pendiente para iniciar una sesión). Se considera que una sesión UDP es medio abierta cuando se detecta tráfico en una sola dirección. (Recuerde que el UDP es un protocolo no orientado a la conexión.)

El CBAC supervisa las sesiones medio abiertas tanto en números absolutos como en tendencias relativas. Una vez cada minuto, el CBAC saca un total de todos los tipos de sesiones medio abiertas y pondera el total con respecto al umbral permitido que se especifica en el archivo config (como opción predeterminada, el límite es 500 solicitudes medio abiertas). Una vez que se excede el umbral, el CBAC comienza a eliminar las solicitudes medio abiertas de su tabla de estado. Seguirá eliminándolas hasta que llegué a un umbral mínimo, donde las operaciones regresarán al estado normal. El fragmento de código siguiente muestra una configuración típica del comando **max-incomplete high**. Es una buena práctica conservar el rango alto-bajo pequeño, para que el CBAC pueda hacer uso frecuente de esta característica de control.

```
Firewall(config)#ip inspect max-incomplete high 1000
Firewall(config)#ip inspect max-incomplete low 900
```

Los comandos inspect one-minute El otro comando para controlar las sesiones medio abiertas es **inspect one-minute**. En lugar de actuar sobre el número de conexiones existentes medio abiertas, lo que se mide es la cantidad de nuevas sesiones medio abiertas. Funciona de una manera muy parecida al comando **max-incomplete**. A continuación se muestra un ejemplo de configuración (con los valores predeterminados):

```
Firewall(config)#ip inspect tcp one-minute high 900
Firewall(config)#ip inspect tcp one-minute low 400
```

Otros comandos TCP Intercept El CBAC cuenta con otros comandos para frustrar los ataques DoS. Como se mencionó antes, el comando **ip inspect tcp synwait-time** controla los ataques SYNflood eliminando las solicitudes de conexión con los bits SYN que han estado pendientes por más tiempo que el límite especificado (30 segundos, como opción predeterminada). De igual manera el comando **ip inspect tcp finwait-time** controla los ataques FINflood (los bits FIN son intercambiados cuando una conexión TCP está lista para cerrarse; su valor predeterminado es de cinco segundos). El comando **ip inspect tcp max-incomplete host** se utiliza para especificar los valores de umbral y tiempo de expiración para la detección DoS específica del host TCP. Éste limita el número de sesiones medio abiertas que se permiten con la misma dirección de destino del host y cuánto tiempo el CBAC seguirá eliminando nuevas solicitudes de conexión desde el host (los valores predeterminados son 50 sesiones medio abiertas y 0 segundos). Por último, la protección genérica se da al configurar los tiempos máximos de inactividad para las conexiones con los comandos **ip inspect tcp idle-time** e **ip inspect udp idle-time** (con los valores predeterminados de 1 hora y 30 segundos, respectivamente).

Firewall PIX Secure de Cisco

Por mucho tiempo, el firewall PIX Secure fue el producto principal de Cisco para tareas de firewall. Como verá un poco más adelante, está siendo desplazado por la Adaptive Security Appliance (ASA, aplicación de seguridad adaptiva) de Cisco (pero parece que va a pasar algo de tiempo antes de que el PIX ya no lo sea). El grupo de características del firewall del IOS está dirigido a clientes más sensibles al precio o para tareas de acordonamiento del acceso dentro de las redes corporativas. Cisco posicionó el PIX para competir mano a mano con los mejores productos firewall del mercado. El firewall PIX difiere del firewall del IOS de las formas siguientes:

- **Hardware/software integrado** El firewall PIX es un paquete integrado en una plataforma de hardware construida para dar servicio pesado de firewall. No viene como un paquete de software independiente.
- **Adaptive Security Algorithm (algoritmo adaptativo de seguridad)** El PIX implementa una inspección del estado y una arquitectura de corte que entrega un alto desempeño, no un filtro de paquetes ni un firewall proxy de aplicación.

NOTA El procesamiento de corte es una técnica que permite que una conexión (HTTP, FTP o Telnet) sea autorizada y permitida una vez que se encuentre en la capa de la aplicación. Luego, todos los paquetes que la sigan, en esa sesión, se filtrarán en la capa de red.

- **Opción VPN integrada** Las redes privadas virtuales tienen soporte nativo; sin embargo, una tarjeta de procesador plug-in configura óptimamente las VPN que soportan la codificación avanzada de Internet Protocol Security (IPSec, seguridad del protocolo de Internet) y los estándares para el Internet Key Exchange (IKE, intercambio de claves de Internet).

Los administradores de red están poniendo cada vez más atención a los dispositivos construidos con un propósito, como el firewall PIX Secure de Cisco, para satisfacer sus necesidades de seguridad en la red. La electrónica y el software en el firewall PIX están diseñados específicamente para lograr el equilibrio entre una avanzada funcionalidad de seguridad y la necesidad de un desempeño de alta capacidad. Al firewall PIX y productos dedicados como éste, se les llama *aparatos de red* (el término de moda para los dispositivos fabricados para servir una función de red escasamente definida). La ventaja más obvia del uso de un aparato firewall es que el software del IOS no tiene que dividir su tiempo entre el filtrado y el enrutamiento.

Más allá del debate entre el aparato y el enrutador habilitado como firewall, Cisco está posicionando el PIX como un sistema integrado en tiempo real contra los aparatos firewall basados en plataformas UNIX de los competidores. El argumento es que los aparatos firewall basados en UNIX deben pagar un precio en desempeño y seguridad. El razonamiento es que un sistema operativo de propósito general UNIX tipo kernel no sólo tiene latencias e información redundante inadecuadas para el trabajo de un firewall, sino que también tiene huecos de seguridad inherentes que los hackers pueden utilizar para irrumpir en el mismo firewall.

Adaptive Security Algorithm (algoritmo adaptativo de seguridad) del firewall PIX

Adaptive Security Algoruthm es, *a grosso modo*, equivalente al Context-Based Access Control (control de acceso basado en el contexto) del firewall del IOS. Ambos sirven como la máquina central para sus respectivos productos de firewall. Esto es benéfico, porque los administradores de red están familiarizados con el ambiente y los comandos básicos (**configure**, **debug**, **write**, etcétera). Pero ASA tiene un conjunto muy diferente de comandos específicos para firewall, y su arquitectura es radicalmente diferente de la del firewall del IOS. ASA permite al firewall PIX implementar medidas de seguridad más estrictas y escalar a tamaños de gateway de mayor capacidad.

NOTA ¿Qué es un algoritmo? Este término puede sonar como si se requiriera conocer física cuántica para escribir uno de ellos, junto con una gran cantidad de ecuaciones cuadráticas. Pero los algoritmos no tienen ningún misterio. Un algoritmo no es más que un conjunto de reglas cuidadosamente diseñadas que se aplican a procesos repetitivos que son capaces de manejar condiciones variables. En efecto, algunos algoritmos contienen ecuaciones matemáticas, pero la mayoría no las tiene. Las computadoras hacen un uso muy extenso de los algoritmos porque casi todos los procesos computacionales son repetitivos y pueden manejarse con variables.

El comando security-level El cliché dice que el mundo no está pintado de blanco y negro sino de gris. De la misma forma, en el mundo de la seguridad de las interconexiones, donde el modelo de los "chicos buenos contra los malos" se queda corto, ya que casi *todo mundo* es considerado como sospechoso. La tendencia en la verdadera seguridad de las redes de alto desempeño, entonces, es la capacidad de designar redes y hosts como un espectro de niveles de seguridad en lugar de solamente como "dentro" o "fuera".

El comando **security-level** del firewall PIX permite especificar niveles relativos de seguridad para interfaces tanto dentro como fuera del firewall. La aplicación de niveles de seguridad relativos, interfaz por interfaz, le permite dibujar un mapa de seguridad mucho más descriptivo del que sería capaz si definiera todas las redes como internas o externas.

Para configurar las interfaces de un firewall con niveles de seguridad relativos, ingrese un comando **security-level** para cada interfaz. Además, debe utilizar el comando **nameif** para identificar la interfaz que desea administrar.

Puede seleccionar cualquier valor para el nivel de seguridad entre 0 y 100, sin que se permita que dos interfaces en un firewall PIX tengan el mismo nivel.

Es una práctica común asignar niveles en decenas, como se muestra en el siguiente fragmento de código, que identifican ocho interfaces en tres zonas de seguridad:

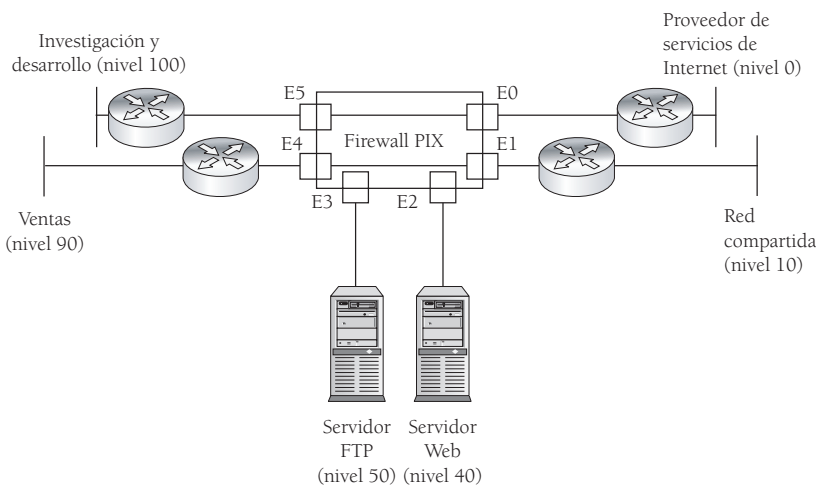
```
firewall(config)# interface gigabitethernet0/0
firewall(config-if)# nameif inside
firewall(config-if)# security-level 100
firewall(config-if)# ip address 10.1.10.10 255.255.255.0
firewall(config-if)# no shutdown
firewall(config-if)# interface gigabitethernet0/1
firewall(config-if)# nameif outside
firewall(config-if)# security-level 0
```

```
firewall(config-if)# ip address 10.1.20.10 255.255.255.0
firewall(config-if)# no shutdown
```

La forma como trabajan los niveles de seguridad es que, como opción predeterminada, *todo* el tráfico con un nivel de seguridad alto es permitido en un nivel de seguridad bajo. En este contexto, la aplicación de reglas se simplifica y el tráfico para un determinado host, por ejemplo, puede utilizar un nivel de seguridad más bajo que el que le fue asignado. El software considera como saliente a una conexión que se está llevando a cabo desde un nivel más alto a una red más baja; considera como entrante a una conexión dirigida de una interfaz de bajo nivel a un nivel alto. Este esquema permite que el administrador de red aplique reglas de una manera mucho más específica.

Debido a que cada zona tiene su propia escala de seguridad, existe la opción de implantar verificaciones de seguridad intrazonales. Por ejemplo, a las listas de acceso podrían aplicársele restricciones en el tráfico que fluye entre los hosts conectados a las dos redes DMZ. Algunos usos posibles de los niveles de seguridad se describen en la figura 7-14.

De la misma forma que con el firewall IOS y otros firewalls, es posible que los paquetes no atraviesen el firewall PIX con una conexión y un estado. El Adaptive Security Algorithm verifica los paquetes entrantes utilizando las reglas siguientes:




```
nameif ethernet0 outside security0
nameif ethernet1 outside security10
nameif ethernet2 dmz security40
nameif ethernet3 dmz security50
nameif ethernet4 inside security90
nameif ethernet5 inside security100
```

Figura 7-14. El comando security-level dibuja un mapa de seguridad más detallado y poderoso.

- Cuando se mueven de un nivel de seguridad alto a uno bajo, todas las conexiones salientes son permitidas, con excepción de las configuradas como negaciones en las listas de acceso saliente.
- Las conexiones estáticas salientes pueden configurarse utilizando el comando **static**, evitando el paso por los conjuntos de traducción dinámica creados mediante los comandos **global** y **nat** o **pat**.

Ranuras de traducción del firewall PIX De la misma forma que con el firewall del IOS, la traducción de direcciones y el rastreo de sesiones se encuentran en el centro de la arquitectura. Pero el firewall PIX utiliza un sistema más formal para implantar la traducción de direcciones IP. En lugar de sólo crear una nueva traducción e ingresarla dinámicamente en una lista de acceso reflexiva, como lo hace el firewall del IOS, la ASA asigna una *ranura* a la nueva conexión.

Para ayudar a administrar el uso de ranuras, puede especificar un límite de ranuras cuando configure interfaces con el comando **nat**. De esta forma, los administradores de red evitan que los usuarios de red individuales consuman demasiadas ranuras de traducción.

NOTA ¿Sabía que algunas aplicaciones utilizan más de una conexión a la vez? Por ejemplo, FTP consume dos conexiones. Un navegador Web (que opera el protocolo de aplicación HTTP) puede consumir cuatro o más conexiones, si se encuentra en el proceso de carga de una página u otros objetos, como los applets de Java. Así que no considere a las conexiones de Internet como algo que el usuario decide iniciar o terminar conscientemente. Las sesiones se inician y se terminan sin que siquiera nos demos cuenta. Se dice que Microsoft Internet Explorer consume ¡hasta 20 conexiones TCP por usuario!

Se verá cómo funciona una simple configuración firewall PIX para mostrar algunos de los comandos. Se han escrito libros completos acerca de firewalls, por lo que sólo abarcaremos los comandos que nos ayudarán a comprender las operaciones básicas del firewall PIX. Éste opera una versión especial del IOS, por lo que se aplican las convenciones usuales del comando IOS. En la figura 7-15 se muestra una configuración PIX con un enrutador de escudo, un enrutador de escudo interior y un servidor DMZ conectado. La configuración incorpora traducción de direcciones globales, restricciones en el tráfico saliente y una ruta estática saliente con un conducto entrante.

NOTA Existe una gran cantidad de firewalls PIX en el mercado que están configurados de manera similar a ésta (la que tenemos aquí le dará una buena idea de lo que se está utilizando). Tenga presente que los comandos están actualizados, los comandos antiguos se han quitado y se han agregado los nuevos a medida que sale un nuevo software. En general, el software de seguridad se actualiza con frecuencia. Siempre consulte la documentación específica para su configuración real de hardware y software.

El primer paso consiste en ingresar al modo de interfaz de configuración, apuntando a cada interfaz como se está configurando:

```
Firewall.enable
Password:******
```

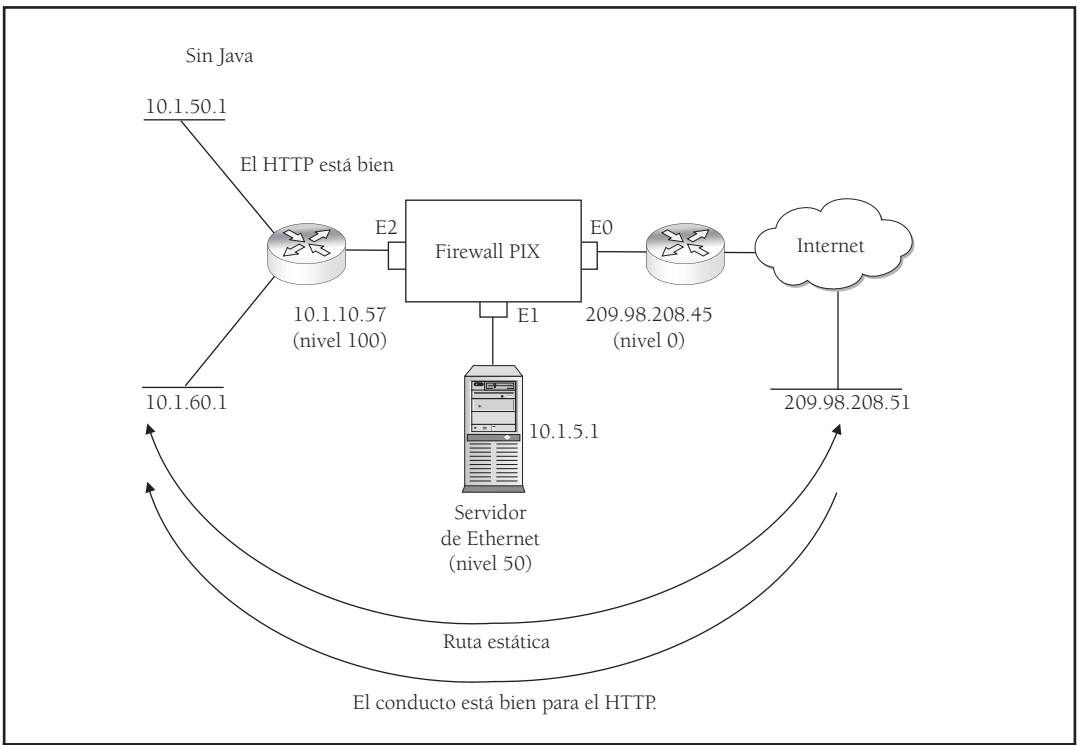


Figura 7-15. Este firewall PIX de tres interfaces soporta una ruta estática con conducto.

```
Firewall#config t
Firewall(config)#
```

Luego, los comandos **interface** se utilizan para proporcionar zonas y niveles de seguridad a las interfaces:

```
Firewall(config)#nameif ethernet0 outside security0
Firewall(config)#nameif ethernet1 Extranet security50
Firewall(config)#nameif ethernet2 inside security100
```

A continuación, los comandos **interface** determinan la especificación Ethernet que las interfaces operarán (autopercepción 10/100 Mbps):

```
Firewall(config)#interface ethernet0 auto
Firewall(config)#interface ethernet1 auto
Firewall(config)#interface ethernet2 auto
```

Las interfaces deben estar identificadas con direcciones IP y con máscaras, lo que se hace utilizando los comandos **ip address**. Observe que se usan los nombres que le acaba

de dar a la interfaz (outside, Extranet e inside) y que las direcciones IP internas privadas se utilizan para la Extranet y dentro de las interfaces (10.1.5.1 y 10.1.10.57):

```
Firewall(config)#ip address outside 209.98.208.45 255.255.255.240
Firewall(config)#ip address Extranet 10.1.5.1 255.255.255.0
Firewall(config)#ip address inside 10.1.10.57 255.255.255.0
```

El comando **nat** se utiliza para permitir que todos los usuarios de dos grupos de usuarios internos efectúen conexiones salientes mediante las direcciones IP traducidas. El número que sigue a los argumentos (**inside**) de las dos instrucciones es un número NAT ID o de referencia NAT (1 y 2), utilizado para vincular grupos a conjuntos de direcciones globales:

```
Firewall(config)#nat (inside) 1 10.0.0.0 255.0.0.0
Firewall(config)#nat (inside) 2 10.0.0.0 255.0.0.0
```

Las instrucciones que utilizan el comando **global** crean dos conjuntos de direcciones globales. Se asignan a usuarios por medio de los nombres ID del NAT (1 y 2, en este caso). La instrucción de la parte media es el conjunto de direcciones PAT. Lo que está pasando aquí es que al sistema se le está indicando que asigne direcciones NAT y, cuando éstas se estén utilizando, comience a aplicar la dirección global PAT a las sesiones. Todas las conexiones asignadas a una dirección PAT mostrarán una dirección de origen igual a 209.98.208.50:

```
Firewall(Config)#global (outside) 1 209.98.208.46-209.98.208.49 netmask
255.255.255.240
Firewall(Config)#global (outside) 1 209.98.208.50 netmask 255.255.255.240
Firewall(Config)#global (outside) 2 209.98.210.1-209.98.210.254 netmask
255.255.255.240
```

Se utiliza una instrucción **static** para crear una dirección IP externamente visible. Una instrucción **conduit** acompañante permite un host o red específicos (un socio de negocios, por ejemplo) a través del firewall PIX. La instrucción de ejemplo siguiente permite que los usuarios de un host externo accedan a través del firewall al servidor 10.1.60.1 mediante conexiones TCP para acceso a Web. La cláusula **eq 80** especifica que la conexión TCP deba operar en el puerto 80 (el número de puerto del protocolo de aplicación http). El modificador **any** permite que cualquier host externo se conecte a 10.1.60.1:

```
Firewall(config)#static (inside, outside) 209.98.208.51 10.1.60.1
                 netmask 255.255.255.0
Firewall(config)#conduit permit tcp host 10.1.60.1 eq 80 any
```

Esta instrucción que utiliza el comando **outbound** crea una lista de acceso que permite el acceso a un host Web interno (puerto 80), pero que le prohíbe descargar applets de Java. El PIX utiliza el comando **outbound** para crear listas de acceso y el comando **apply** para aplicarlas. Observe que el número de puerto de Java se representa por la cadena de texto **java** en lugar de un número de puerto. Es posible utilizar nombres en lugar de números en algunos protocolos nuevos de la capa de aplicación, como Java. Obviamente es mucho más fácil recordar nombres en lugar de números codificados. La opción **outgoing_src** niega o permite que una dirección interna tenga la capacidad de iniciar conexiones salientes utilizando los servicios especificados en el comando **outbound**:

```
Firewall(config)#outbound 10 permit 209.98.208.22 255.255.255.255 80
Firewall(config)#outbound 10 deny 209.98.208.22 255.255.255.255 java
Firewall(config)#apply (Extranet) 10 outgoing_src
```

Existen muchos otros comandos que pueden utilizarse cuando estamos configurando un firewall PIX. En realidad, en casi todos los ambientes de conectividad existen algunos más que *deben* configurarse para que el firewall trabaje de manera adecuada. La configuración apropiada de un firewall PIX con múltiples servidores, protocolos, listas de acceso y enrutadores de protección podría llevar días. Las configuraciones posibles podrían ser interminables. Pero las instrucciones simples que revisamos aquí demuestran que configurar un firewall (uno de los dispositivos más complejos de la conectividad) no es cosa del otro mundo. Puede volverse un poco laborioso, pero hacerlo sólo es cosa de ir interfaz por interfaz y comando por comando.

PIX OS 7.2 La última versión del software del IOS firewall PIX es la 7.2, y ésta ofrece gran variedad de mejoras y actualizaciones con respecto a las versiones de software anteriores. Algunas de sus características incluyen:

- ▼ **Inspección y control de la aplicación** Permite mayor control y capacidad sobre la inspección de paquetes, disminuyendo la probabilidad de ataques y proporcionándole la capacidad de inspeccionar paquetes para varios servicios.
- ■ **Acceso remoto y VPN sitio por sitio** Las capacidades VPN se mejoran en la versión 7.2 e incluyen la validación de igual a igual y las funciones mejoradas de seguridad.
- ■ **Integración de la red** Las redes se conectan más fácilmente gracias a las nuevas capacidades de integración. Por ejemplo, el OS 7.2 del PIX incluye las capacidades del Point-to-Point Protocol over Ethernet (PPPoE, protocolo punto a punto sobre Ethernet) que permite más fácilmente que las computadoras conectadas por medio de un ISP utilicen conexiones de banda ancha. También incluye el soporte del DNS Dinámico así como mejoras del enrutamiento multidirigido.
- ■ **Capacidad de recuperación y escalabilidad** La confiabilidad se refuerza con mejoras a la capacidad de recuperación y escalabilidad. La detección de fallas en cuestión de milisegundos permite la detección y recuperación de un sistema en menos de un segundo, mientras que el Standby ISP Support permite que su red detecte fallas en un ISP de respaldo en el caso de que el primer ISP falle.
- ▲ **Administración y facilidad de servicio** La administración ha mejorado con características como el comando traceroute, que permite rastrear la ruta de un paquete hasta su destino, y el comando de rastreo de paquetes, que permite analizar el paquete a medida que circula por el aparato. El OS 7.2 del PIX también incluye mejoras en el manejo del direccionamiento IPv6.

Existen muchos otros aspectos importantes en la configuración de un firewall. Un ejemplo es la configuración de dos firewalls (uno como servidor de gateway principal y el otro como dispositivo de respaldo en línea al que se dirigirá el tráfico en caso de que el servidor principal falle, que se configura utilizando el comando **failover**). Otro ejemplo es la configuración del firewall para integrarlo con un servidor secundario, como el TACACS+.

Marcas y modelos

No importa cuál firewall necesite, Cisco ofrece su línea PIX en cinco distintas variedades. En el extremo inferior de la escala se encuentra el Cisco Secure PIX Firewall 501. Este modelo está dirigido al mercado de la pequeña oficina/oficina en casa, y está equipado con un procesador a 133 MHz, con conexiones Ethernet y con escasos 16 MB. En el otro extremo del espectro se encuentra el gigante de los firewalls. Debieron nombrar Gigawall al Cisco Secure PIX Firewall 535, porque todo en este firewall parece como que gritara en voz alta "giga". Está dirigido al mercado empresarial y de proveedores de servicios, y cuenta con un procesador de 1 GB, una RAM de 1 GB y conexiones Gigabit Ethernet.

Aunque estos firewall parecen muy diferentes, comparten la funcionalidad primordial del firewall PIX (entre otras, su integración de hardware y software, la funcionalidad VPN y la extensibilidad). En la tabla 7-2 se muestra una comparación entre la línea Secure PIX Firewalls de Cisco.

	Secure PIX Firewall 501 de Cisco	Secure PIX Firewall 506E de Cisco	Secure PIX Firewall 515E de Cisco	Secure PIX Firewall 525 de Cisco	Secure PIX Firewall 535 de Cisco
Mercado	Oficina pequeña/oficina en casa	Oficina remota/sucursal	Negocios y empresas de tamaño pequeño a mediano	Corporativos y proveedores de servicios	Corporativos y proveedores de servicios
Procesador	Intel Pentium a 133 MHz	Intel Pentium a 300 MHz	Intel Pentium a 433 MHz	Intel Pentium III a 600 MHz	Intel Pentium III a 1 GHz
RAM	16 MB	32 MB	64 MB	Hasta 256 MB	1 GB
Interfaces	Cinco puertos, Fast Ethernet	10/100 BaseT Fast Ethernet de Integración Doble	Soporta hasta seis interfaces 10/100 BaseT Fast Ethernet	Soporta hasta ocho Fast Ethernet 10/100 BaseT o tres interfaces Gigabit Ethernet	Soporta hasta 14 10/100 BaseT Fast Ethernet o nueve interfaces Gigabit Ethernet

Tabla 7-2. Línea de Secure PIX Firewalls de Cisco (*continúa*).

	Secure PIX Firewall 501 de Cisco	Secure PIX Firewall 506E de Cisco	Secure PIX Firewall 515E de Cisco	Secure PIX Firewall 525 de Cisco	Secure PIX Firewall 535 de Cisco
Conexiones	Transmisión de datos a 60 Mbps; 7 500 conexiones concurrentes; 10 túneles VPN simultáneos.	Transmisión de datos a 100 Mbps; 25 000 conexiones concurrentes; 25 túneles VPN simultáneos.	Transmisión de datos a 190 Mbps; 130 000 conexiones concurrentes; 2 000 túneles VPN simultáneos.	Transmisión de datos a 330 Mbps; 280 000 conexiones concurrentes; 2 000 túneles VPN simultáneos.	Transmisión de datos a 1.7 Gbps; 500 000 conexiones concurrentes; 2 000 túneles VPN simultáneos.
Soporte de NIC	Fast Ethernet	Fast Ethernet	Fast Ethernet	Fast Ethernet, Gigabit Ethernet	Gigabit Ethernet, Fast Ethernet

Tabla 7-2. Línea de Secure PIX Firewalls de Cisco (*conclusión*).

Aparatos adaptativos de seguridad

Mientras que los firewalls PIX han sido la parte medular de las herramientas de seguridad de Cisco, la novedad es su Adaptive Security Appliance (ASA, aplicación de seguridad adaptativa). ASA es el componente primordial en la red de autodefensa de Cisco.

ASA está diseñada para asegurar una organización entera, sin importar el tamaño de ésta. Además, puede asegurar un segmento de un negocio, mientras que consolida los mecanismos de seguridad y reduce los costos de operación.

La serie ASA 5500 de Cisco proporciona las siguientes características basadas en red:

- ▼ Prevención de virus y gusanos.
- ■ Prevención de spyware y adware.
- ■ Inspección del tráfico de la red.
- ■ Prevención de hackers.
- ▲ Prevención de negación del servicio.

Estas características vienen agrupadas con la correlación de eventos de seguridad en el dispositivo.

La seguridad de la aplicación proporciona la inspección y el control para proteger dinámicamente las aplicaciones de negocios en red. Estos servicios incluyen el control de servicios de igual a igual que consumen un gran ancho de banda y mensajería instantánea, control de acceso URL, protección de aplicaciones de negocios y gran número de protecciones específicas para la aplicación de VoIP y multimedia. Los dispositivos ASA de Cisco pueden

funcionar como clientes VPN de hardware, simplificando la administración, junto con los servicios VPN y SSL acelerados por hardware.

Las ASA se administran mediante los servicios del Cisco ASA Software 7.2. La última versión del software incluye 50 nuevas mejoras de seguridad; algunas de las más importantes son el fortalecimiento de los servicios del firewall de la capa de la aplicación y la integración de los servicios de Cisco Network Admission Control (NAC, control de la admisión en la Red).

Los servicios de firewall de la capa de la aplicación ayudan a proteger las aplicaciones, incluido Web, correo electrónico, VoIP, mensajería instantánea y protocolos de conectividad de Microsoft. El NAC incluye el análisis de usuarios y dispositivos, al verificar las actualizaciones del software de seguridad y de sistemas operativos antes de que se les otorgue el acceso a la red.

Existen cinco modelos en la línea ASA, mismos que se comparan en la tabla 7-3.

Característica	ASA 5505 Base/Security Plus	ASA 5510 Base/Security Plus	ASA 5520	ASA 5540	ASA 5550
Mercado	Pequeños negocios, sucursales, SOHO	Pequeños negocios y empresas pequeñas	Pequeñas empresas	Empresas medianas	Empresas grandes
Transferencia de datos	150 Mbps	300 Mbps	450 Mbps	650 Mbps	1.2 Gbps
Número de conexiones de sitio a sitio y de acceso remoto	10/25	250	750	5 000	5 000
Número de conexiones VPN SSL	25	250	750	2 500	5 000
RAM	256 MB	256 MB	512 MB	1 024 MB	4 096 MB
Puertos	Conmutador de ochos puertos Fast Ethernet con dos puertos Power sobre Ethernet	Ocho Fast Ethernet con un puerto de administración	Cuatro Gigabit Ethernet con un puerto de administración	Cuatro Gigabit Ethernet con un puerto de administración	Ocho Gigabit Ethernet con un puerto de administración

Tabla 7-3. Línea de aparatos de seguridad adaptativa de Cisco (*continúa*).

Característica	ASA 5505 Base/Security Plus	ASA 5510 Base/Security Plus	ASA 5520	ASA 5540	ASA 5550
Característica de seguridad	Seguridad de la capa de aplicación, firewall transparente de la capa 2 e IPSec	Seguridad de la capa de aplicación, firewall transparente de la capa 2 e IPSec	Seguridad de la capa de aplicación, firewall transparente de la capa 2 e IPSec, agrupamiento de VPN y balanceo de cargas	Seguridad de la capa de aplicación, firewall transparente de la capa 2 e IPSec, agrupamiento de VPN y balanceo de cargas	Seguridad de la capa de aplicación, firewall transparente de la capa 2 e IPSec, agrupamiento de VPN y balanceo de cargas
Anti-X (antivirus, antispyware, bloqueo de archivos, antispam, antiphishing y filtrado de URL)	No	Sí	Sí	Sí	No

Tabla 7-3. Línea de aparatos de seguridad adaptativa de Cisco (*conclusión*).

REDES PRIVADAS VIRTUALES

¿Qué es una red privada virtual (VPN, Virtual Private Network)? Como sucede muy a menudo en el negocio de las computadoras, la propaganda publicitaria puede meter desorden en lo que de otra forma sería un término claro. En el caso de las VPN, existe confusión acerca de qué es *virtual* en una VPN, ¿la privacidad o la red? A continuación se presenta la definición en dos partes de una red privada virtual:

- La topología de la VPN opera principalmente sobre una infraestructura de red *compartida*, generalmente Internet, y tiene al menos un segmento LAN privado en cada extremo.

▲ Las sesiones de VPN operan a través de un conexión codificada.

Para funcionar a través de conexiones codificadas por Internet, los segmentos de red en cada extremo de la VPN de sitio a sitio deben estar bajo el control administrativo de la empresa (o las empresas) que operan la red virtual. En términos prácticos, esto significa que los enrutadores de los extremos deben estar bajo un régimen común operativo y de seguridad. Ante todo, los enrutadores en los puntos extremos de una VPN deben trabajar bajo un esquema de codificación común.

Tradicionalmente, la conectividad de larga distancia a una interconexión ha dependido de una WAN con una línea arrendada. Además, una línea arrendada simplemente no es una opción para una persona que viaja mucho y no puede estar en un lugar por mucho tiempo para que se justifique una línea arrendada. A continuación se exponen algunas razones por las que las VPN están causando impacto en el mercado de las líneas arrendadas:

▼ **Costos menores** Las líneas arrendadas requieren equipo muy costoso de espina dorsal y ancho de banda para el transporte. Además, las VPN no necesitan equipo terminal ni módems de acceso en las instalaciones.

■ **Movilidad de la red** Relativamente hablando, los vínculos VPN son sencillos y no muy costosos de instalar, cambiar o mover. Debido a esto, la infraestructura de las comunicaciones de la organización no tendrá que sufrir cambios significativos cuando se instale, reconfigure o quite una VPN. Además, la disponibilidad de Internet asegura que puede conectar su VPN casi en donde quiera.

▲ **Acceso** Debido a su disponibilidad, los suscriptores de cualquier parte de la VPN tienen el mismo nivel de acceso y de vista a los servicios centrales (como correo electrónico, sitios Web externos e internos, seguridad, etcétera).

¿Qué compone una VPN?

Considere a las VPN como redes de área amplia que trabajan, al menos parcialmente, mediante redes no seguras como Internet. Como pasa en casi todas las WAN, una VPN podría proporcionar una mezcla de tipos de acceso, como se muestra en la figura 7-16.

Las VPN están reemplazando, de manera constante, el papel que juegan las WAN en la conectividad empresarial. Toda o una parte de una VPN puede ser una intranet, una extranet o un vehículo de acceso remoto para trabajadores móviles o que viajan lejos. Un número muy importante de nuevas VPN pertenecen y son operadas por proveedores de servicios de Internet, quienes dividen el ancho de banda de las VPN entre las empresas. Ofrecer el servicio de proveeduría externa de VPN se está convirtiendo en una práctica común, sobre todo en las grandes empresas, porque es menos costoso y la empresa puede depender del ISP para administrar la infraestructura de las VPN para ellos.

El cifrado y otras medidas de seguridad definen en gran medida una VPN. Esto es por la simple razón de que operar WAN empresariales a través de Internet es fácil y no muy costoso, pero no es factible sin la seguridad apropiada. Por tanto, la seguridad es parte de lo que conforma una VPN. También está definida por un grupo de servidores de acceso compatibles con Internet, dispositivos de red (como firewalls) y técnicas de administración de la conectividad.

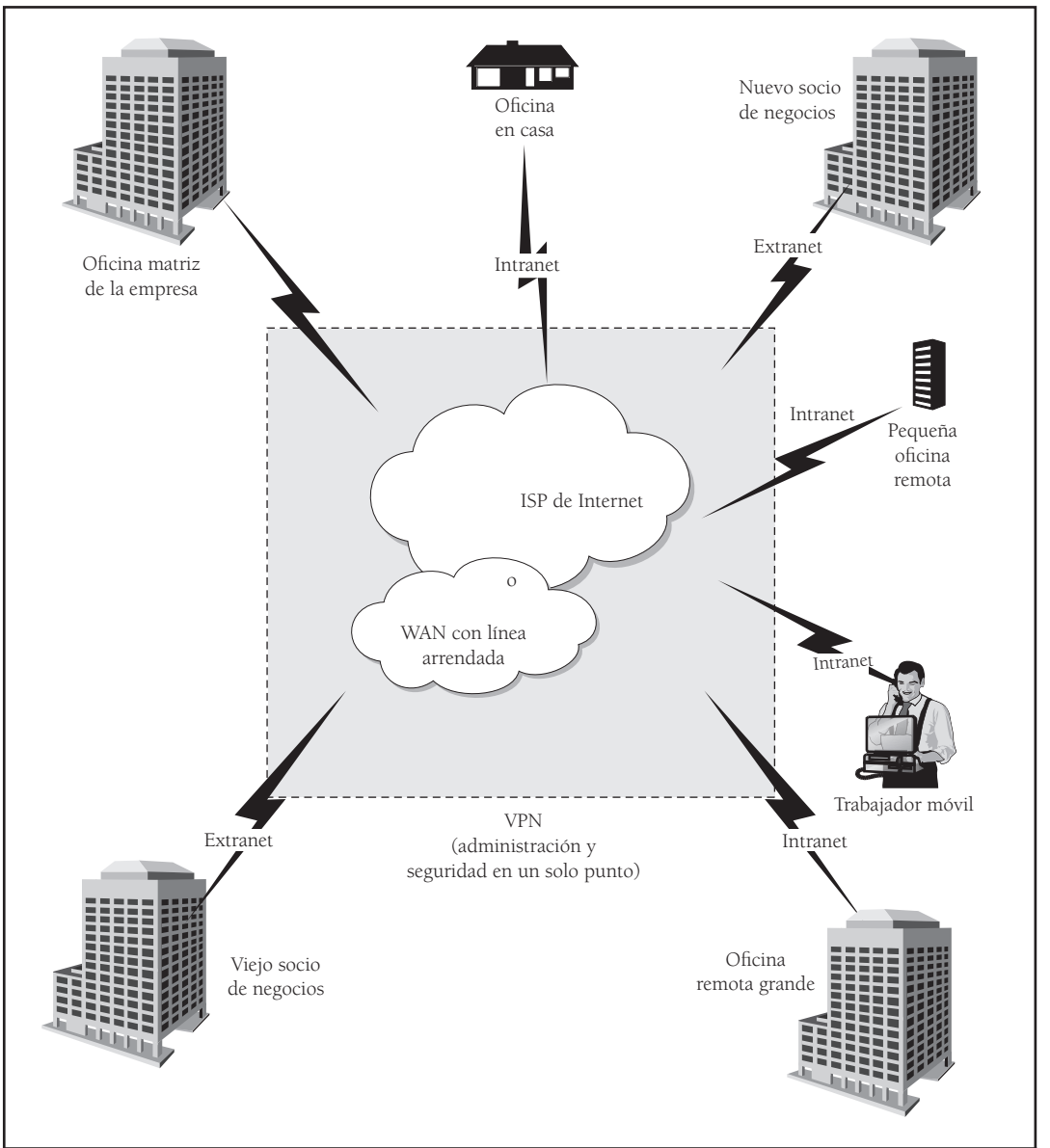


Figura 7-16. Las VPN son WAN cifradas que vienen en varios estilos.

NOTA La codificación es una técnica que mezcla en forma aleatoria el formato de los datos de tal forma que sólo puedan leerse con un sistema que tenga una clave autorizada con una fórmula matemática necesaria para ordenar los datos. (Los encabezados de paquetes se dejan ordenados, de tal forma que puedan enrutarse.) En el contexto de nuestro análisis en esta sección del libro, el cifrado y descifrado se lleva a cabo entre dos enrutadores de cifrado de igual a igual, llamados enrutadores de igual a igual. (Observe que los firewalls pueden también manejar el cifrado.) Los enrutadores de igual a igual comparten una clave de algoritmo secreta utilizada para ordenar los datos. Los enrutadores de igual a igual deben autentificarse entre sí antes de cada sesión codificada utilizando las claves del Digital Signature Standard (DSS, estándar de firma digital), que son cadenas de caracteres únicos. Cuando se verifica una firma, el enrutador de igual a igual es autentificado y puede comenzar la sesión codificada. La mezcla aleatoria en realidad se hace utilizando una clave temporal de Data Encryption Standard (DES, estándar de cifrado de datos), que debe intercambiarse en los mensajes de conexión entre los enrutadores de igual a igual. Cuando la sesión codificada termina, se elimina la clave DES.

Los componentes que conforman una VPN son:

- **Túnel** Conexiones punto a punto a través de una red IP de conexión no orientada (en esencia, un conjunto de saltos predeterminados de enrutador que se toman a través de Internet para garantizar el desempeño y la entrega).
- **Cifrado** Es la mezcla aleatoria del contenido de un paquete IP (pero generalmente no el encabezado) para hacerlo ilegible a todos, con excepción de quienes cuenten con una clave para ordenarlo. (Las claves sólo las tienen los emisores y receptores de la VPN.)
- **Encapsulado** Es la colocación de un marco dentro de un paquete IP como puente entre redes que no sean similares (el paquete IP se desempaqueta en el otro lado), permitiendo que el efecto de túnel se lleve a cabo en lo que de otro modo serían segmentos incompatibles de red VPN.
- **Autentificación de paquetes** Es la capacidad de asegurar la integridad de un paquete VPN, confirmando que su contenido (carga útil) no ha sido alterado en toda la ruta.
- **Autentificación del usuario** Son las capacidades de autentificación, autorización y contabilidad (AAA) del usuario que se imponen a través de los servidores de seguridad, como TACACS+, RADIUS o Kerberos.
- **Control de acceso** Son los firewalls, los dispositivos de detección de intrusión y los procedimientos de auditoría de seguridad utilizados para supervisar todo el tráfico que cruza el perímetro de seguridad de las VPN.
- **Calidad del servicio (QoS)** El QoS de Cisco es un conjunto de estándares y funciones de administración de interconexiones que aseguran la interoperabilidad de los dispositivos y las plataformas de software y para apoyar la plataforma con el fin de garantizar el desempeño y la confiabilidad de la red de extremo a extremo.

Esta lista muestra cómo una VPN impone una seguridad *limpia*. Si se forzara a los administradores de red o a los usuarios a que siguieran varios pasos para cumplir con tareas simples, el uso de una VPN sería incosteable y poco seguro. Por tanto, en términos prácti-

cos, una VPN debe configurarse utilizando dispositivos de software y hardware con estas características.

La solución de Cisco

Para entregar la funcionalidad VPN, Cisco ha diseñado una solución completa con el fin de poner su nombre en alto. En lugar de concentrarse solamente en el aspecto de hardware del problema, Cisco desarrolló una solución integral que depende tanto del hardware como del software.

La solución de Cisco no puso todos sus huevos VPN en una sola canasta. Además de los enrutadores y los firewalls PIX habilitados con funciones VPN, cuentan con software especialmente diseñado para utilizar esa funcionalidad extra. Las secciones siguientes se dedican al software y hardware de Cisco y a la manera en que ambos se utilizan de manera conjunta para diseñar VPN para acceso remoto, intranets y extranets.

Hardware

Para entregar la funcionalidad VPN, Cisco ha diseñado características VPN en un gran número de sus modelos de enrutadores. Por ejemplo, el Cisco 1721 VPN Access Router se utiliza para conectar sitios remotos pequeños con una VPN. El 1721 está diseñado para llevar a cabo el cifrado a alta velocidad y entregar servicios de enrutamiento de túnel en un mismo paquete. Las VPN tradicionalmente han sido soluciones basadas en software. Sin embargo, al tener presente el diseño de equipo para la funcionalidad VPN, se han mejorado los servicios VPN sobrepasando a las soluciones de software. Por ejemplo, al agregar la funcionalidad VPN a los enrutadores de las series 2600 y 3600 de Cisco, ésta es diez veces mayor que las soluciones de software independientes.

En la tabla 7-4 se presenta una lista con parte del hardware de Cisco que cuenta con la característica de VPN.

Producto	Descripción
Concentrador de la Serie VPN 3000 de Cisco	Acceso remoto, escalable, diseñado para empresas. Cuenta con hasta 100 Mbps codificados con 3Des.
Firewalls Secure PIX de Cisco	Cifrado integrado por software; hasta 425 Mbps de utilización codificada.
Enrutadores de la Serie 800 de Cisco	Para el mercado de pequeña empresa y oficina casera, hasta 128 Kbps para ISDN, de banda ancha.
Enrutadores de la Serie 1700 de Cisco	Para el mercado de oficina pequeña, hasta T1/E1.

Tabla 7-4. Parte del hardware de Cisco habilitado para VPN (*continúa*).

Producto	Descripción
Enrutadores de la Serie 2600 de Cisco	Para el mercado de sucursales, hasta dos T1/E1.
Enrutadores de la Serie 3600 de Cisco	Para sucursales de gran tamaño, conectividad T1/E1 escalable.
Enrutadores de la Serie 3800 de Cisco	Para sucursales de gran tamaño, conectividad T1/E1 escalable.
Dispositivos para la Seguridad Adaptiva de la Serie ASA 5500 de Cisco	Para negocios de mediano tamaño, diseñado para contrarrestar un gran número de amenazas de seguridad.

Tabla 7-4. Parte del hardware de Cisco habilitado para VPN (*conclusión*).

Cliente VPN de Cisco

A pesar de que Cisco está construyendo funcionalidad VPN en su hardware, no han olvidado el aspecto de software en la solución. La solución VPN de Cisco puede empezar en una pieza de equipo que no tenga conexión hacia una pieza de hardware de Cisco. Cuando se instala la versión 4.8 de Secure VPN Client de Cisco en una PC basada en Windows, un empleado que trabaja en casa, una oficina remota o un viajero puede conectarse a través de cualquier interconexión con su propio túnel VPN.

El cliente (que puede colocarse en una PC en cualquier lugar del mundo) cuyo tráfico atraviesa Internet como cualquier otro tráfico, encuentra su camino a su enrutador base o firewall PIX.

Requisitos El cliente VPN está disponible en Windows 9*x*, NT, 2000, Millennium Edition, XP, 2003 Server y Vista. El cliente también opera sobre el OS X de Mac, Linux y Solaris.

La instalación es un proceso sencillo que consiste en hacer doble clic en un icono en el CD-ROM de instalación. Una vez que está instalado el cliente, permanece en un icono, en la parte inferior de la pantalla, hasta que se necesite.

Características Bajo la superficie, el cliente VPN de Cisco cuenta con varias herramientas diseñadas para proporcionar un túnel IPSec estable y seguro. Dentro de algunas de sus características principales se incluyen:

- El administrador de la red puede exportar y bloquear la directiva de seguridad.
- El cliente cumple con el IPSec. También soporta:
  - Seguridad en modo de túnel o de transporte.
  - Algoritmos DES, 3DES, MD-5 y SHA-1.
  - IKE utilizando ISAKMP/Oakley Handshake and Key Agreement.

- Es compatible con casi todos los dispositivos de comunicación de Windows, incluidos adaptadores LAN, módems, tarjetas PCMCIA, etcétera.
- Está configurado de manera central para facilidad de uso.
- Es compatible con las Autoridades de Certificados X.509, en las que se incluyen:
  - Servicios de Certificación Windows 2000.
  - Verisign en sitio.
  - Sistema de Administración de Certificados de Netscape.
  - GUI para que la directiva de seguridad y la administración de certificados sea amigable al usuario.
- ▲ Es transparente cuando está en su uso.

Excavación de un túnel

Cuando se tiene una combinación de hardware y software habilitados para VPN de Cisco, es cuando se hace evidente la fortaleza de la solución VPN de Cisco. Por ejemplo, con el uso de un Cisco Secure PIX 515E Firewall junto con el software PIX 7.2, el PIX puede originar o terminar túneles VPN entre dos PIX, entre un PIX y cualquier enrutador habilitado para VPN de Cisco, y entre un PIX y el Secure VPN Client de Cisco.

Los escenarios siguientes explican cómo pueden satisfacerse diferentes necesidades de VPN.

Acceso remoto La VPN más básica se presenta cuando un usuario necesita acceder a la red desde un lugar remoto. Por ejemplo, si un vendedor se encuentra de viaje y necesita acceder a información que se encuentra en la red de su compañía, sólo necesita iniciar una VPN de regreso a su oficina base.

Observemos cómo puede hacerse una conexión de acceso remoto. En la figura 7-17 se muestra la oficina matriz de una compañía de alimentos para mascotas ubicada en San Pablo, Veracruz, y un vendedor que se encuentra en viaje de negocios en Mérida, Yucatán. Para acceder a la red de su compañía, el usuario remoto se conectará a través de un túnel seguro que se encuentra establecido a través de Internet. Lo anterior permite que el vendedor acceda a la información interna como si su computadora estuviera físicamente conectada a la LAN corporativa.

En la figura 7-18, se agregan los elementos de hardware que permitirán construir la VPN.

En este escenario, utilizamos un firewall PIX como dispositivo VPN en el extremo de la compañía. Este mismo escenario puede configurarse con un enrutador en lugar del firewall PIX. Utilizando la misma construcción, uno de los enrutadores con características VPN de Cisco podría utilizarse en lugar del PIX.

Nota: vuelva a consultar la tabla 7-4 para encontrar una lista del hardware con característica VPN de Cisco.

Evidentemente, sus necesidades de conectividad y sus medios económicos determinarán en gran medida su decisión entre un firewall PIX y un enrutador. Para una máxima seguridad, debe utilizar el firewall. Un enrutador o un concentrador con características VPN habilitadas proporcionan un desempeño mejorado con respecto a las soluciones VPN que sólo se basan en software.

Esta configuración funciona bien para el escenario del "agente viajero", pero la funcionalidad VPN puede también establecerse entre dos compañías o entre una compañía y una sucursal.

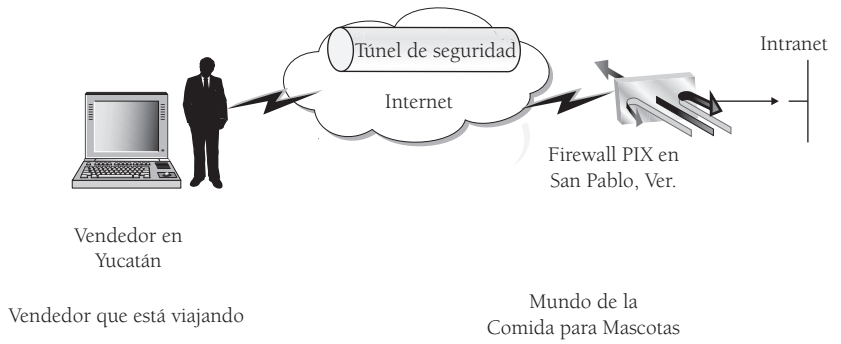


Figura 7-17. Un usuario remoto utiliza una VPN para acceder a su red corporativa.

Acceso de sitio a sitio Aun en un ambiente donde una WAN sea el modo predilecto de conectividad, se pueden conseguir ahorros sustanciales empleando una VPN. Las VPN de sitio a sitio extienden el alcance de una WAN típica reemplazando a las redes privadas existentes por medio de líneas arrendadas, Frame Relay o ATM para conectar a socios de negocios y a sucursales con el sitio central.

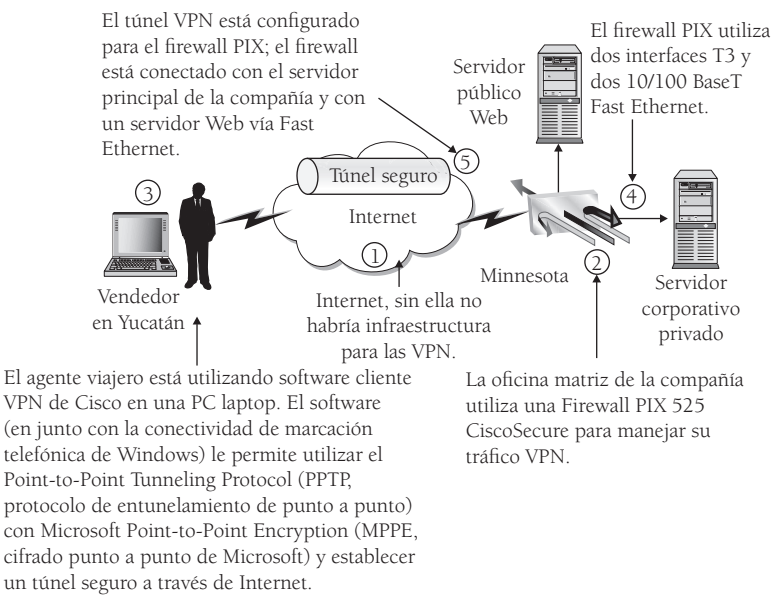


Figura 7-18. Éstos son los componentes de hardware de una conexión VPN con acceso remoto.

En esta capacidad, las VPN no modifican los requisitos de las WAN privadas, como el soporte de varios protocolos, la confiabilidad y la cobertura. En cambio, las VPN cumplen con estos requisitos, pero son más eficientes y flexibles. Para entregar capacidades del tipo de una WAN privada bajo un presupuesto, las VPN de sitio a sitio utilizan Internet o proveedores del servicio de Internet mediante entunelamiento y cifrado para efectos de privacidad y, en algunos casos, calidad del servicio para una mejor confiabilidad. El escenario siguiente muestra cómo puede establecerse una VPN entre la oficina matriz de una compañía y una oficina remota (intranet) o entre dos socios de negocios (extranet).

En este ejemplo, se mostrará cómo dos socios de negocios pueden vincular sus respectivas redes por medio de Internet. En la figura 7-19 se muestra la casa matriz de HydroDynamics, que necesita proporcionar acceso de extranet a su socio, Johnson Pneumatics. Las dos oficinas están conectadas mediante un túnel IPSec seguro, que se conecta a través de Internet. Los empleados de Johnson Pneumatics pueden acceder al servidor Web de su socio de negocios por todo el país. En la figura 7-20 se muestran los detalles de hardware y software del vínculo VPN entre HydroDynamics y Johnson Pneumatics.

Como se observa, la conexión de dos socios de negocios o de una sucursal a través de una VPN es mucho más fácil y menos costosa que una WAN. Por medio de un túnel seguro a través de Internet, se puede lograr la conectividad sin consumir muchos recursos de la compañía.

ENRUTADORES DE ACCESO

El acceso a su red puede darse de varias formas. Como se estudió en la sección anterior, los servidores de acceso, por ejemplo, satisfacen las necesidades de marcación telefónica. Sin embargo, tal vez las sucursales, las pequeñas oficinas, los empleados remotos y el personal que viaja necesiten un desempeño mayor y un acceso más robusto a la red. Como tal, el acceso a estas conexiones puede proporcionarse utilizando enrutadores de acceso, que son un subconjunto de los productos enrutadores de Cisco.

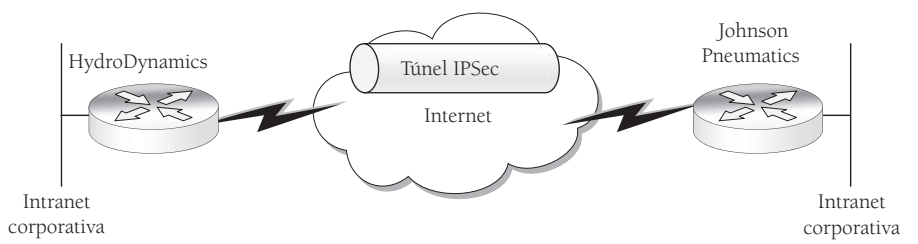


Figura 7-19. Los socios de negocios pueden utilizar las VPN para vincular sus organizaciones.

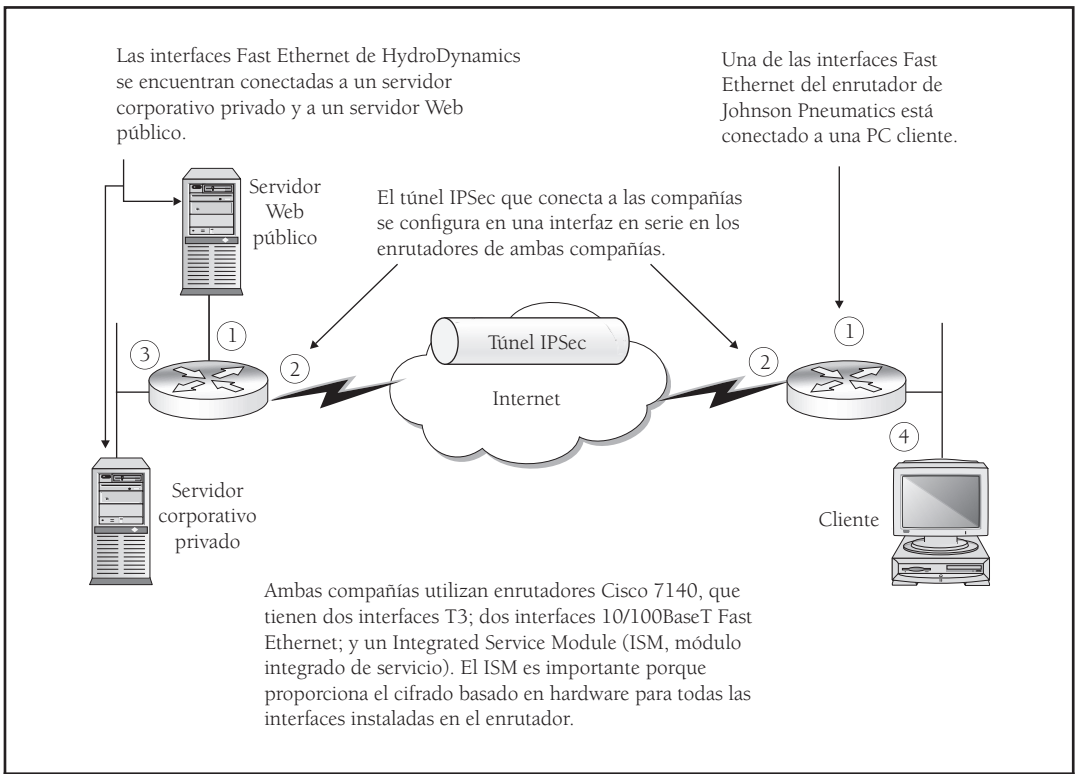


Figura 7-20. Éstos son los componentes de hardware de una solución VPN de sitio a sitio.

Panorama general

La línea de enrutadores de acceso de Cisco proporciona funcionalidad a los empleados remotos que necesitan un acceso más eficiente a la red. Para facilitar estas conexiones, los enrutadores de acceso incluyen características de seguridad reforzada y de desempeño. Los enrutadores de acceso ofrecen acceso seguro a Internet y a la red a través de una gran variedad de tecnologías de acceso WAN de alta velocidad. Entre los beneficios de los enrutadores de acceso se encuentran:

- ▼ Acceso de banda ancha de alta velocidad y acceso por línea arrendada.
- ■ Aplicaciones de varios servicios para la integración de voz/datos.
- ■ Capacidades integradas de seguridad, con VPN IPSec, un firewall de inspección de estado y la detección de intrusos.
- ▲ Los modelos de extremo superior son modulares, proporcionando flexibilidad en su diseño y uso.

La línea de enrutadores de acceso de Cisco abarca una gran gama de necesidades en las organizaciones, ofreciendo modelos para su uso desde pequeñas oficinas y oficinas caseras, hasta negocios de tamaño mediano y empresas de gran tamaño.

Además de realizar las tareas convencionales, los enrutadores de acceso proporcionan una seguridad mejorada, una mejor administración y la calidad de servicio (QoS) necesarios para aplicaciones como videoconferencia, aprendizaje electrónico, VPN y colaboración en línea.

Una característica importante de los enrutadores de acceso es su capacidad de QoS. Puesto que a los enrutadores se les solicitará el envío de VoIP, contenido multimedia y otras aplicaciones que están a expensas de la latencia de paquetes, el QoS es un mecanismo necesario. Estas capacidades dan como resultado conversaciones y transmisiones más regulares y sin problemas de fluctuaciones.

Modelos

Cisco ofrece gran variedad de enrutadores de acceso con varios niveles de características. Los enrutadores de acceso de nivel superior tienen una configuración fija (es decir, simplemente se conectan a una WAN, como una línea DSL). Sin embargo, cuando comienza a ascender por la escalera de los productos de enrutamiento de Cisco, existen más oportunidades para la modularidad. Pueden configurarse para funcionar en una conexión OC-3 o T1, por ejemplo, dependiendo de las tarjetas y módulos que utilice para configurarlo.

Cisco ofrece ocho modelos de enrutadores de acceso en dos series:

- ▼ La serie 1700 de enrutadores de acceso de Cisco está dirigido a los negocios pequeños y medianos. Esta serie, con seis módulos, proporciona gran cantidad de capacidades VPN IPSec, de firewall de estado y detección de intrusos.
- ▲ La serie 3700 de enrutadores de acceso de Cisco proporciona dos modelos: los enrutador de Acceso multiservicio 3725 y 3745. Éstos son parte integral de la AVVID de Cisco (Architecture for Voice, Video, and Integrated Data, arquitectura para voz, video y datos integrados). Puesto que éstos utilizan el IOS, son muy configurables y ofrecen QoS y características de seguridad a las sucursales.

CONJUNTO DE ADMINISTRACIÓN DE LA SEGURIDAD DE CISCO

Las amenazas contra la seguridad abundan en Internet, en formas muy diferentes. Ya sea que provengan de virus, hackers o ataques de negación del servicio, el administrador de la red ha tenido que mantenerse firme para evitar problemas. Con el fin de aliviar estos problemas, la seguridad se ha convertido en una cuestión de poner parches (las VPN se utilizan para una cosa y los firewalls para otra). La Security Management Suite de Cisco tiene como objetivo agrupar a todos los aspectos de seguridad, de tal manera que puedan administrarse desde un punto central, en lugar se hacerlo como hasta ahora.

El conjunto está formado por dos componentes:

- ▼ Cisco Security Manager (CSM).
- ▲ Monitoring, Analysis, and Response System (MARS, monitoreo, análisis y sistema de respuesta) de Cisco Security.

Cisco Security Manager

El CSM proporciona la administración de la seguridad utilizando diferentes vistas. Una vista con base en el dispositivo le permitirá visualizar todos los dispositivos de una red, además de las directivas que puedan establecerse y administrarse en cada uno de ellos. La visión de la directiva del ASM permite la creación y la administración de directivas con base en las necesidades específicas de la organización.

Esto no sólo permite que se puedan establecer directivas en la organización; si llegaran a existir puntos delicados específicos dentro de la misma, que requirieran una mayor atención, podría establecerse y manejarse. Además, el administrador de red también puede establecer directivas en varios vínculos de la red.

El CSM también proporciona una vista centrada en la topología, que ofrece una representación visual de la red, la cual tiene conexiones a los mapas de la red, permitiendo al administrador manejar las directivas desde este nivel. Estas vistas le ofrecen al administrador una estructura integrada para administrar los servicios de seguridad como los firewalls, las VPN y el servicio de prevención de intrusiones.

MARS de Cisco Security

Cisco Security MARS reúne, relaciona y reporta eventos de seguridad de dispositivos Cisco y otros fabricantes. Cuando se presenta un evento, el CS-MARS proporciona información acerca del incidente, en qué parte de la red ocurrió y la mejor forma de atacarlo.

La versión 4.2 de CS-MARS incluye características para la categorización y vista de eventos en tiempo real y dinámicamente. El tráfico inusual se puede identificar por medio de filtros en tiempo real de los datos correspondientes a eventos de seguridad.

Utilizando el Security Manager de Cisco, el administrador puede identificar el dispositivo y la directiva que son responsables de la negación del tráfico sospechoso. Esto va dirigido a proteger la red, asegurar la disponibilidad y reducir los costos.

Existe gran cantidad de formas de administrar el acceso a su red (instalando un servidor de acceso para usarse con marcación telefónica o un enrutador de acceso para el tráfico a Internet). Sin importar qué seleccione, es de vital importancia que tenga presente el factor seguridad, y una red debe tener un firewall y un IDS configurados apropiadamente en el sitio para frustrar cualquier acción proveniente de personas maliciosas.

CAPÍTULO 8

Soluciones inalámbricas de Cisco

Por convención, la conectividad se ha logrado conectando cables en los equipos electrónicos y, después, dejando volar a los paquetes. Pero una de las adiciones más significativas y actuales a la interconectividad proporciona a los paquetes la facilidad de contar con sus propias alas. Dichos paquetes ya no necesitan estar restringidos por el límite físico que representa el cableado de par trenzado. La era de la conectividad inalámbrica ha llegado y está entre nosotros.

INTRODUCCIÓN A LA CONECTIVIDAD INALÁMBRICA

Con todos los avances en la conectividad alámbrica convencional, sólo fue cuestión de tiempo antes de que alguien volteara al cielo y se preguntara: "¿Qué hay acerca del medio inalámbrico?" La verdad sea dicha, alguien se hizo esa pregunta hace más de una década, pero el resultado práctico y funcional a esa pregunta se ha hecho realidad en el último par de años.

En esta sección, echamos un vistazo al pasado para ver de dónde viene la conectividad inalámbrica, cómo funciona y de qué manera le puede beneficiar.

Las raíces de la conectividad inalámbrica

Para comprender mejor la conectividad inalámbrica actual, es importante conocer su historia y cómo hemos llegado a donde estamos.

La tecnología LAN más popular en el mundo es Ethernet. El Institute of Electrical and Electronic Engineers (IEEE) lo define con el estándar 802.3. Ethernet ofrece una norma de conectividad de alta velocidad disponible casi en todos lados y que evoluciona de manera constante. En sus inicios, Ethernet ofrecía velocidades de transferencia de datos de 1 Mbps y después de 10 Mbps, que crecieron después a 100 Mbps y a 1 Gbps, y actualmente se encuentran a 10 Gbps. Debido a que el IEEE 802.3 es una norma abierta, existe una amplia gama de proveedores y productos para los usuarios de Ethernet. La norma asegura cierto nivel de interoperabilidad, sin importar de qué producto o fabricante se trate.

Las primeras tecnologías Wireless LAN (WLAN, LAN inalámbricas) no eran tan veloces como Ethernet en ese entonces. Trabajaban en la banda de 900 MHz y a una velocidad de sólo 2 Mbps como máximo. Además, eran de propietario por naturaleza, lo que eliminaba toda comunicación entre productos de diferentes fabricantes. A pesar de estos obstáculos, la conectividad inalámbrica logró forjar un nicho respetable en mercados verticales como la venta al menudeo y en almacenes. Fue muy útil en esos ambientes, porque la movilidad y la flexibilidad de la tecnología era necesaria en ambientes donde los trabajadores utilizaban dispositivos portátiles en actividades como la administración de inventarios y la recolección de datos.

Aironet, una compañía de conectividad inalámbrica, se dio cuenta de esta necesidad y comenzó a presionar para el establecimiento de estándares en 1991.

NOTA Cisco compró Aironet en el 2000 y utiliza su tecnología como parte medular de sus productos WLAN. En este capítulo se hablará acerca de la compra de Cisco y sus dispositivos de Aironet.

Aironet argumentaba que mediante el establecimiento de estándares, las LAN inalámbricas ganarían una amplia aceptación en el mercado. Al año siguiente, los desarrolladores

de WLAN comenzaron a trabajar en productos que trabajaban en la banda de frecuencias sin licencia de 2.4 GHz. Esta nueva tecnología fue muy atractiva en dos mercados en particular:

- **Cuidado de la salud** La conectividad inalámbrica hizo posible la transferencia de información relacionada con el paciente a dispositivos móviles de cómputo. En lugar de tener que cargar una computadora de un cuarto de operaciones a otro, la conectividad inalámbrica coloca la información del paciente en las manos de un profesional de la salud.
- **Escuelas** Al no estar restringida por cables, hizo posible que las escuelas que fueron construidas sin tubos de cableado (recuerde esos días), instalaran redes de computadoras sin tener que hacer agujeros en las paredes e instalar cables entre los pisos del edificio.

En junio de 1997, fue desarrollada la tecnología que sirve como estándar medular para las WLAN que conocemos ahora. El IEEE liberó la norma 802.11 para la conectividad de área local inalámbrica. Dicha norma soporta la transmisión de datos mediante luz infrarroja y dos tipos de transmisión de radio dentro de la banda de frecuencias sin licencia de 2.4 GHz: Frequency Hopping Spread Spectrum (FHSS, espectro extendido de saltos de frecuencia) y Direct Sequence Spread Spectrum (DSSS, espectro extendido de secuencia directa).

NOTA Analizaremos el estándar 802.11 más adelante en este capítulo.

Beneficios

Si la simple capacidad de desempeñar funciones de conectividad sin estar atado a un conmutador o un concentrador no es suficiente para conmoverlo, miremos más de cerca las capacidades de la transmisión de datos inalámbrica, junto con algunas situaciones en que la conectividad inalámbrica representa un beneficio.

Qué puede hacer

Además del aspecto "vaya, esto es estupendo" de una computadora que trabaja sin cables, existe gran cantidad de factores importantes que hacen de la conectividad inalámbrica una tecnología productiva y útil:

- **Movilidad** Con las WLAN, los usuarios pueden tener acceso en tiempo real a su LAN desde casi cualquier lugar (dependiendo de su rango, los obstáculos y la interferencia). Esta capacidad aparece sin tener que estar conectado con cables a la red. Esta movilidad permite a los usuarios la libertad de acceder a la red casi desde cualquier lugar y a cualquier hora.
- **Costo de propiedad reducido** A pesar de que los costos de hardware para el arranque de una WLAN son más elevados que el de una LAN convencional, cuando se consideran los gastos totales del ciclo de vida, la inversión que representa una WLAN puede ser mucho menor. Los beneficios mayores a largo plazo en cuanto al costo, se reflejan en ambientes más dinámicos, donde se presentan más cambios y movimientos.
- **Escalabilidad** Las WLAN pueden configurarse fácilmente en gran variedad de topologías de red para satisfacer las necesidades de instalaciones y aplicacio-

nes específicas. Las configuraciones son muy flexibles, pueden modificarse muy fácilmente y pueden ir desde simples redes de igual a igual que son ideales para pocos usuarios, hasta redes que cuentan con toda la infraestructura para miles de usuarios que permiten la función de moverse en un área amplia.

- **Transferencia de datos a alta velocidad** Las velocidades de transmisión de las WLAN están comenzando a ser comparables con las de las redes alámbricas. Los usuarios pueden acceder a información a 54 Mbps, lo que está a la par con las velocidades convencionales por medios alámbricos. Aunque todavía no alcanzan velocidades de 100 Mbps, 1 Gbps y 10 Gbps que se pueden lograr con las redes alámbricas, las inalámbricas tienen una velocidad respetable y funcional.
- **Interoperabilidad** Los fabricantes (como Cisco) que construyen sus productos utilizando el estándar 802.11 aseguran su funcionalidad dentro de la red con otros equipos o marcas que cumplen con el estándar.
- **Cifrado para la seguridad de las LAN de alta velocidad** Mediante la incorporación de los esquemas WPA y WPA2, puede garantizarse la seguridad de la red. El WPA/WPA2 brinda servicio a puntos de acceso (AP), tarjetas PC e ISA y adaptadores PCI.
- **Velocidad y simplicidad de instalación** Antes de que apareciera la tecnología inalámbrica, para conectar computadoras a una LAN era necesario instalar y conectar un montón de cables en completo desorden. La tarea se complicaba aún más si el cableado necesitaba atravesar paredes o ir de un piso a otro. La tecnología inalámbrica simplifica y acelera el proceso de instalación.
- ▲ **Flexibilidad de instalación** Debido a que las WLAN no están restringidas por las barreras físicas que tienen las LAN alámbricas, pueden proporcionar acceso a la red a usuarios y estaciones de trabajo donde la conexión de una LAN es simplemente imposible.

Aplicaciones

Dado el continuo cambio de la tecnología y sus aplicaciones, resulta una barbaridad encasillar una tecnología en particular en campos específicos. Sin embargo, la siguiente lista le proporciona una idea de la manera de utilizar la tecnología inalámbrica en gran variedad de campos. De nuevo, esta lista no debe considerarse una extensión de las capacidades inalámbricas, sus propias circunstancias y situaciones serán su mejor guía para determinar si se beneficiará más de una tecnología alámbrica o una inalámbrica:

- ▼ **Empresarial** Con una WLAN, los empleados empresariales ya no necesitarán estar atados a sus escritorios. Utilizando laptops equipadas con NIC (Network Interface Cards, tarjetas de interfaz de red) inalámbricas, los empleados pueden aprovechar totalmente los servicios de correo electrónico, compartir archivos y navegar en Web, sin importar el lugar de la oficina o el campus de la empresa en que se encuentren.
- **Servicios y venta al menudeo** Los servicios de servicios (como los restaurantes) pueden utilizar las WLAN para tomar y enviar órdenes de alimentos a la cocina desde la mesa. Las tiendas de venta al menudeo pueden utilizar las WLAN para configurar cajas registradoras temporales para eventos especiales, como el día posterior a Navidad o al comienzo de una venta.

- **Manufactura** Las WLAN conectan estaciones de trabajo de una fábrica y dispositivos de recolección de datos a la red de una compañía. Se pueden mover a lo largo del piso y no requieren de más cableado en el piso de una fábrica.
- **Bodegas** Las WLAN conectan terminales de cómputo portátil y montadas sobre una base con lectores de código de barras y enlaces inalámbricos de datos. Esta tecnología se utiliza para ingresar y conservar la ubicación del inventario de una bodega.
- **Educación** Escuelas, colegios y universidades se benefician de la conectividad móvil permitiendo que estudiantes, profesores y equipo administrativo que cuenten con computadoras notebook se puedan conectar a la red académica institucional para recibir clases, y a Internet, para navegar por Web y acceder al servicio de correo electrónico. Más aún, la tecnología inalámbrica puede hacer que haya más espacios para las clases al permitir que los laboratorios de cómputo portátiles sean una realidad.
- **Finanzas** Las personas de finanzas pueden utilizar una PC portátil con un adaptador WLAN para recibir información sobre precios desde una base de datos en tiempo real y para acelerar y mejorar la calidad de las transacciones.
- **Cuidado de la salud** Mediante el uso de PC portátiles inalámbricas, los profesionales del cuidado de la salud pueden acceder a información en tiempo real e incrementar la productividad y la calidad del cuidado a pacientes reduciendo los retrasos en los tratamientos, la necesidad de ir de paciente en paciente y eliminando el papeleo redundante a la vez que reduciendo los errores de transcripción.

Esto es sólo la punta del iceberg sobre los usos de la conectividad inalámbrica. Seguramente, a medida que la tecnología cambie la forma de hacer negocios, irán apareciendo cada vez más usos.

WLAN

Una WLAN es una LAN a la que puede accederse sin tener que estar físicamente atado a un servidor, conmutador, concentrador o cualquier otro dispositivo de conectividad. Utilizando la tecnología de radiofrecuencia (RF), las WLAN transmiten y reciben datos a través del espacio libre, eliminando la necesidad de conexiones cableadas convencionales. Las WLAN se están haciendo cada vez más populares en gran cantidad de ambientes especializados, entre los que se incluye el cuidado de la salud, la venta al menudeo, la manufactura, el almacenamiento de bienes y la academia. Estos ambientes se han beneficiado del aumento en la productividad que representa el uso de PC portátiles y computadoras notebook para transmitir y recibir información en tiempo real hacia y desde una red centralizada. Las WLAN están ganando reconocimiento como una solución de conectividad de red de propósito general para gran variedad de usuarios de negocios.

En esta sección, miraremos más de cerca cómo la conectividad inalámbrica se utiliza de manera práctica. Más adelante, estudiaremos algunas de las tecnologías medulares que están impulsando a las redes inalámbricas. Por último, observaremos nuestra bola de cristal y trataremos de predecir hacia dónde se dirigirá la conectividad inalámbrica en el futuro.

Cómo trabajan

Como los teléfonos inalámbricos, las WAN utilizan las ondas electromagnéticas de radio para transmitir información de un lugar (su laptop, por ejemplo) a otro (un punto de

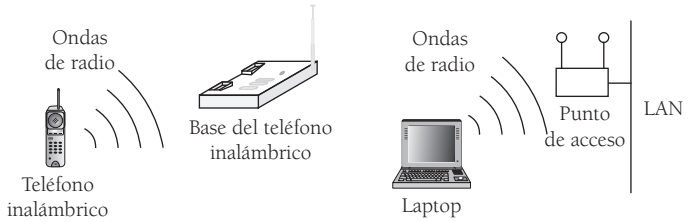


Figura 8-1. Las WLAN transmiten información como los teléfonos inalámbricos.

acceso), sin utilizar un medio físico para transferir el mensaje. En la figura 8-1 se muestra lo anterior.

NOTA A menudos a las ondas de radio se les conoce como portadores de radio, porque su función consiste en entregar energía a un receptor remoto. Los datos transmitidos se montan en el portador de radio, por lo que puede extraerse en el extremo receptor. A esto se le conoce como modulación del portador por la información transmitida.

Una vez que se han agregado los datos en el portador de radio, la señal de radio se expande, ocupando más de una sola frecuencia. Esto sucede debido a que la frecuencia (o velocidad de los bits) de los datos modulados se suma a la del portador.

Esto podría representar un problema, sobre todo en ambientes donde varias computadoras estarán tratando de acceder al dispositivo inalámbrico. Sin embargo, en realidad varios portadores funcionan bien en la misma área, siempre y cuando las ondas de radio sean transmitidas en diferentes frecuencias. Para recolectar datos, el receptor de radio se sintoniza en una sola frecuencia, como se muestra en la figura 8-2, ignorando a las demás.

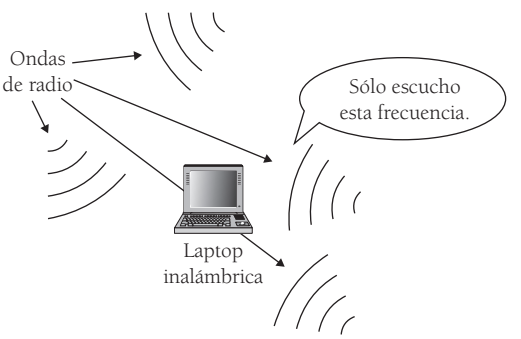


Figura 8-2. Los dispositivos inalámbricos se sintonizan a una sola frecuencia rechazando las demás.

En una WLAN, el dispositivo que se conecta físicamente a la LAN alámbrica es un transceptor (una combinación de transmisor y receptor) y se conoce comúnmente con el nombre de *punto de acceso*. El punto de acceso recibe, almacena y transmite datos entre la WLAN y la red alámbrica. Como se muestra en la figura 8-3, también se puede considerar a un punto de acceso como un concentrador inalámbrico (un solo punto de acceso puede servir a cientos de clientes). En función al rango del punto de acceso, los clientes se pueden ubicar dentro de algunos centímetros o hasta 450 metros de distancia. En condiciones óptimas, la antena del punto de acceso podría estar ubicada a una altura considerable. Sin embargo, la antena podría ubicarse en cualquier lugar que el espacio lo permita.

Para conectarse al punto de acceso, las computadoras cliente utilizan adaptadores WLAN, que son pequeñas tarjetas de PC para computadoras notebook y palmtop, y tarjetas de expansión en computadoras de escritorio. También pueden estar integradas dentro de las computadoras portátiles y en muchas de las nuevas notebooks, palmtops y Tablet PC. Estas tarjetas cuentan con antenas y componentes transceptores.

Arquitectura

Las LAN inalámbricas pueden ser muy sencillas (dos computadoras comunicándose entre sí) o complejas (cientos de computadoras ubicadas en un solo lugar, conectándose con otras computadoras situadas en otro edificio localizado a kilómetros de distancia). Veamos las tres formas básicas por medio de las cuales puede instalar sus redes inalámbricas.

Figura 8-3. Los puntos de acceso sirven como concentradores inalámbricos que conectan uno (o muchos) dispositivos inalámbricos a la LAN.

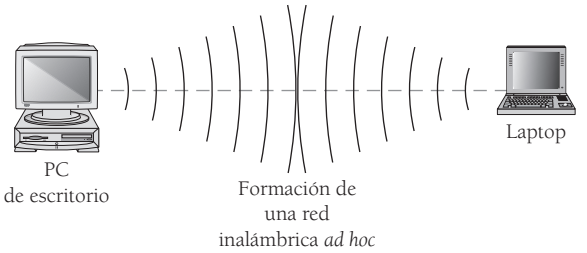


Figura 8-4. Las redes de igual a igual o *ad hoc* conectan dispositivos independientes entre sí.

Igual a igual

La red inalámbrica más básica y sencilla está integrada al menos por dos PC equipadas con tarjetas adaptadoras inalámbricas. Como se muestra en la figura 8-4, no se necesita un punto de acceso; siempre que estas dos computadoras se encuentren dentro del rango de cada una de ellas, formarán su propia red independiente. A esto se le llama *red de igual a igual* o *red ad hoc*. Es muy simple instalar y echar a funcionar redes por demanda como ésta. No requieren administración o preconfiguración; sin embargo, en este caso, cada computadora sólo tendrá acceso a los recursos de la otra, pero no al servidor central o a Internet.

Este tipo de red es ideal para redes caseras o para pequeños negocios que requieran conectividad espontánea.

En el edificio

De la misma forma que las redes alámbricas convencionales, el equipo WLAN en el edificio consta de una tarjeta para PC, una Personal Computer Interface (PCI, interfaz para computadora personal) y adaptadores para cliente Industry-Standard Architecture (ISA, arquitectura estándar de la industria), además de puntos de acceso.

Como se muestra en la figura 8-5, para extender el rango de su WLAN o incrementar la funcionalidad, los puntos de acceso pueden utilizarse en la topología de red y también pueden funcionar como un puente a una red Ethernet alámbrica.

Aplicando la tecnología WLAN a los sistemas de escritorio, se le puede dar a una organización la flexibilidad que es simplemente imposible proporcionar con una LAN convencional. Los clientes pueden desplegarse en lugares donde la instalación de un cable es simplemente imposible. Además, los clientes pueden volverse a ubicar en cualquier lugar y a cualquier hora. Esto hace que la tecnología inalámbrica sea ideal para grupos de trabajo temporales u organizaciones con rápido crecimiento.

La instalación de un punto de acceso puede extender el rango de una red inalámbrica. En esencia, duplica el rango en que los dispositivos se pueden comunicar. Debido a que el punto de acceso está conectado directamente a la red alámbrica, cada cliente tiene acceso a los recursos del servidor y a otros clientes; la cantidad exacta depende del número de transmisiones que estén involucradas y de su naturaleza. Es muy común que los puntos de acceso manejen hasta 50 clientes.

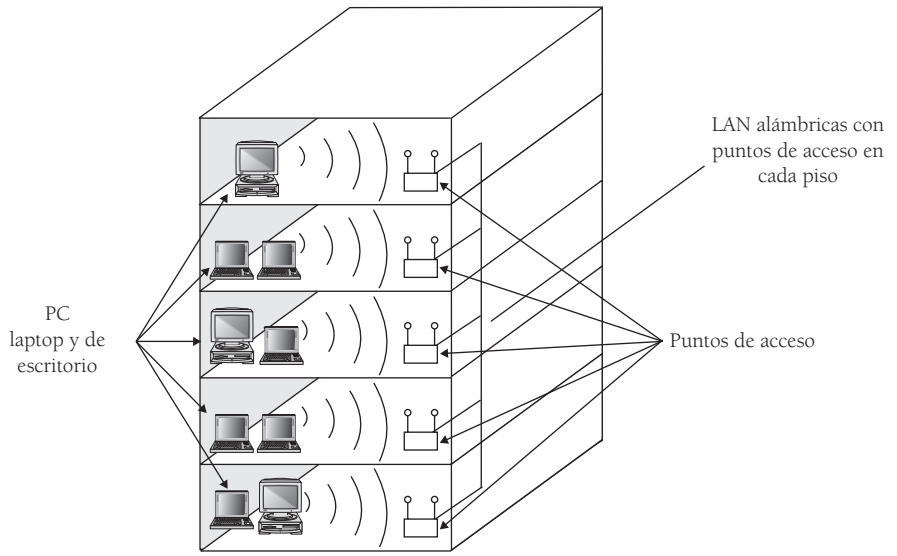


Figura 8-5. Con varios puntos de acceso puede aumentarse la disponibilidad de la LAN.

NOTA Sin embargo, tome en cuenta que a medida que se conectan más clientes a un punto de acceso, éstos reducen la cantidad de tráfico que un punto de acceso puede manejar. Si maneja 40 clientes, no espere que sea tan veloz como uno que esté siendo utilizado por 10 clientes solamente.

Los *repetidores*, como se muestra en la figura 8-6, tienen la apariencia y trabajan como puntos de acceso, pero hay una excepción importante (no están conectados a una red alámbrica). Los repetidores extienden el rango de la red, enviando señales de un cliente a un punto de acceso o a otro repetidor. Los repetidores son necesarios porque las señales se

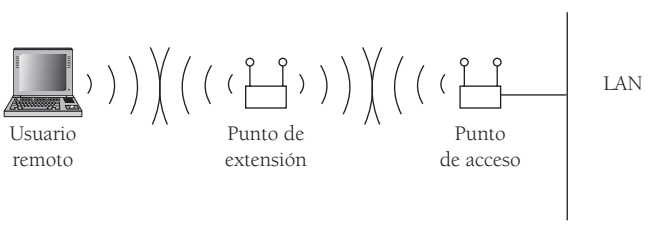


Figura 8-6. Los repetidores son simples puntos de acceso que se configuran para extender el rango de una WLAN.

debilitan a medida que están más alejadas de sus puntos de recepción. Si tiene clientes que estén lejos de la red alámbrica, es posible conectar repetidores para enviar los datos de los clientes a un punto de acceso.

De edificio a edificio

El último logro de la conectividad inalámbrica viene cuando las redes se extienden entre edificios ubicados en diferentes ciudades. Mediante un puente inalámbrico, es posible conectar, como si fueran una sola red, distintas redes ubicadas en edificios a kilómetros de distancia entre sí.

Cuando se conectan las redes entre edificios con cobre o fibra, se presenta gran cantidad de obstáculos que pueden representar el fracaso de un proyecto. Los caminos, los ríos y la política pueden acabar con un proyecto. Un puente inalámbrico hace que las barreras físicas e ideológicas no representen un problema. La transmisión a través del aire de acuerdo con el estándar 802.11 no requiere licencia ni derecho de vía.

Para despliegues que no ofrezcan una alternativa inalámbrica, en forma rutinaria las organizaciones regresan a las tecnologías WAN. Sin embargo, alquilar una línea de un proveedor de servicio telefónico representa un gran número de problemas:

- ▼ La instalación es cara y su configuración toma mucho tiempo.
- ▲ Las cuotas mensuales son elevadas, en el caso de un ancho de banda considerable. El problema adicional es que por los estándares LAN, las velocidades WAN son muy bajas. Esto se debe a que las líneas telefónicas se diseñaron y construyeron para voz y no para datos.

No se puede comprar e instalar un puente inalámbrico en una sola tarde, y su costo es comparable a la instalación de un T1. Es más, no hay cuota mensual (una vez que se hace una conexión inalámbrica), no hay cargos recurrentes. Además, los puentes inalámbricos proporcionan ancho de banda a partir de una tecnología con raíces en los datos y no en la voz.

Para hacer realidad su red de edificio a edificio, necesita dos antenas direccionales y una línea de visión clara entre ellas. Supongamos que tiene una WLAN en el edificio A (la casa matriz) y quiere extenderla a una oficina satélite en el edificio B, que se encuentra a 16 kilómetros del A, en una ciudad vecina. Como se muestra en la figura 8-7, podría instalar una antena direccional en la azotea de cada edificio, y colocar cada antena apuntando hacia la otra. La antena del edificio A se encuentra conectada a su LAN principal mediante un punto de acceso. La antena del edifico B está conectada en forma similar a un punto de acceso hacia esa LAN. Esta configuración agruparía las dos LAN, ubicadas a kilómetros de distancia entre sí, en una sola LAN.

Debido a su movilidad y facilidad de instalación, las WLAN tienen una ventaja significativa sobre las LAN convencionales. Proporcionan oportunidades de conectividad que no se encuentran disponibles en las redes alámbricas, además de que no son demasiado caras a largo plazo.

Tecnologías

Existe gran cantidad de tecnologías que hacen que la transmisión y recepción de datos sea factible. Muchas de ellas tienen sus raíces en la telefonía celular, mientras que otras han sido diseñadas únicamente teniendo presente la conectividad inalámbrica.

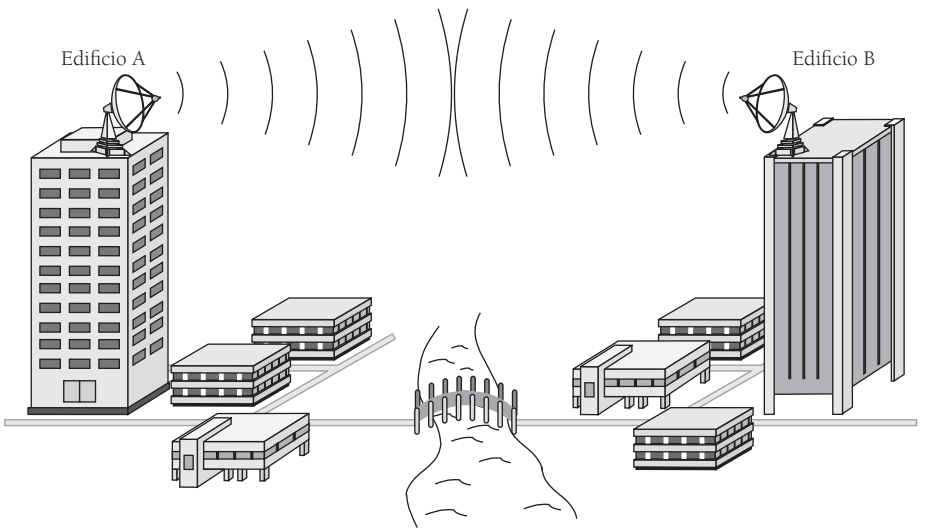


Figura 8-7. Los puentes inalámbricos pueden conectar dos redes ubicadas a kilómetros de distancia.

En esta sección, echaremos una mirada cercana a tres de las tecnologías más populares y al impacto que éstas tienen en sus necesidades de conectividad inalámbrica. Estas tecnologías abarcan la comunicación de datos de corto alcance, la transferencia de datos de largo alcance y cómo puede accederse a Internet utilizando teléfonos celulares.

802.11

La tecnología central que permite que las WLAN se comuniquen es el estándar IEEE 802.11. El grupo de trabajo IEEE 802.11 fue formado a principios de la década de 1990 para desarrollar una norma global para las LAN inalámbricas que operaban en la banda de frecuencia sin licencia de 2.4 GHz. Como ya se mencionó, las primeras versiones de la 802.11 trabajaban a velocidades de hasta 2 Gbps.

El estándar 802.11*x* brinda diferentes variaciones en el protocolo para varias velocidades, frecuencias de operación y alcances. La LAN 802.11*x* está basada en una arquitectura similar al diseño de las redes de telefonía celular. Las LAN inalámbricas (WLAN) funcionan conectando un punto de acceso al servidor, mientras que las computadoras cliente se conectan mediante adaptadores inalámbricos. Estas tarjetas adaptadoras pueden instalarse en las computadoras laptop y de escritorio, y también en otros dispositivos de conectividad, incluidos los servidores de impresión. Muchas laptops incluyen características inalámbricas integradas.

Existen tres tipos de redes 802.11*x* pertinentes a nuestro análisis:

- **802.11a** Utilizando esta especificación, los dispositivos transmiten a 5 GHz y envían datos hasta de 54 Mbps. A pesar de que la velocidad es buena, el rango de la 802.11a sufre de problemas porque está limitada a algún valor cercano a 25 metros en un ambiente típico.

- **802.11b** Con esta especificación, los dispositivos transmiten a 2.4 GHz y envían datos hasta 11 Mbps. Fue la primera red inalámbrica disponible comercialmente. La velocidad no era muy elevada, pero hizo factible la conexión de dispositivos sin que éstos se encontraran unidos mediante cableado Cat 5. Encontrará el estándar 802.11b en dispositivos convencionales, porque está siendo reemplazada por el estándar 802.11g, que es más veloz.
- **802.11g** Esta especificación maneja las comunicaciones de datos de hasta 54 Mbps y utiliza la misma frecuencia que los dispositivos 802.11b (2.4 GHz). Debido a que trabaja en la misma frecuencia, 802.11g permite actualizar de forma fácil desde un norma existente de 802.11b.
- ▲ **802.11n** Es la última versión de la especificación inalámbrica 802.11n. Hasta la fecha de la escritura de este libro, la 802.11n es completamente nueva y el soporte de Cisco a esta norma se presenta ya en algunos de sus productos Linksys. Maneja velocidades hasta 12 veces mayores a la del estándar 802.11g y cuatro veces su alcance.

NOTA Existen otras variaciones alfabéticas del estándar 802.11*x* (802.11c, 802.11d, etcétera hasta 802.11i). Sin embargo, estas versiones en realidad no tienen nada que ver con el estado actual de la conectividad inalámbrica de Cisco.

Para una mejor comprensión de estos tres protocolos y la manera en que se pueden apilar uno sobre el otro, en la tabla 8-1 se muestran sus similitudes y diferencias.

Estándar	802.11a	802.11b	802.11g	802.11n
Velocidad	54 Mbps	11 Mbps	54 Mbps	540 Mbps
Costo	Moderadamente cara	Barata	Más costosa que la 802.11b, pero menos cara que la 802.11a	Es la opción más cara, especialmente a medida que nuevos productos ingresan al mercado
Frecuencia	5 GHz (esta banda no está saturada y puede coexistir con las redes 802.11b y g)	2.4 GHz (esta banda está saturada y puede presentarse interferencia con teléfonos inalámbricos, hornos de microondas y otros dispositivos)	2.4 GHz (esta banda está saturada y podría presentarse interferencia con teléfonos inalámbricos, hornos de microondas y otros dispositivos)	2.4 GHz (esta banda está saturada y puede presentarse interferencia con teléfonos inalámbricos, hornos de microondas y otros dispositivos)

Tabla 8-1. Los atributos de las redes 802.11a, b, g y n (*continúa*).

Estándar	802.11a	802.11b	802.11g	802.11n
Alcance	De 7.5 a 23 metros en interiores	De 30 a 45 metros en interiores	De 30 a 45 metros en interiores	50 metros en interiores
Compatibilidad con radiofrecuencia	Incompatible con las redes 802.11b y g	Es la de uso más extendido	Funciona con la 802.11b, pero es incompatible con la 802.11a	Funciona con las redes 802.11b y g; es una buena forma para aumentar de tamaño las redes existentes

Tabla 8-1. Los atributos de las redes 802.11a, b, g y n (*conclusión*).

Existen dos formas diferentes de configurar una red 802.11 WLAN:

- ▼ *Ad hoc.*
- ▲ Infraestructura.

Echemos un vistazo más detallado a cada uno de los tipos de infraestructura WLAN.

Ad hoc En la red *ad hoc*, las computadoras se conectan para formar una red que funcione como parche, como una red de igual a igual. Como se muestra en la figura 8-8, no existe una estructura jerárquica en la red y no es necesario un punto de acceso. Todo es móvil y cada nodo puede comunicarse con todos los demás. Un buen ejemplo de esto en el mundo real es pensar en una reunión en la que todos los asistentes tuvieran su propia laptop.

Infraestructura El segundo tipo de conexión, que se muestra en la figura 8-9, está muy relacionado directamente con una topología LAN convencional. Este diseño utiliza puntos de acceso fijos a la red mediante los cuáles los nodos móviles pueden comunicarse entre sí. Los puntos de acceso pueden estar ubicados de tal forma que estén dentro de la cobertura, para expandir el alcance de la red.

Diseño 802.11

El estándar 802.11 se desarrolló teniendo presente tres necesidades:

- ▼ La necesidad de una especificación para el control de acceso al medio (MAC) y una capa física para la conectividad inalámbrica de estaciones fijas portátiles y móviles.
- ■ La necesidad de conectividad inalámbrica con máquinas automáticas, equipo o estaciones que requieran de una conectividad rápida.
- ▲ La necesidad de ofrecer una norma global.

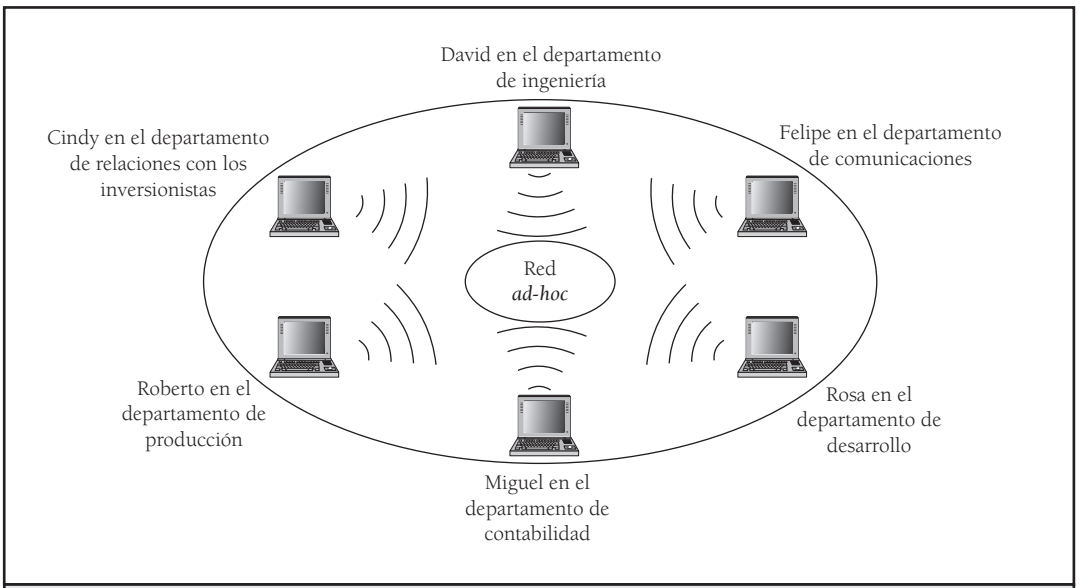


Figura 8-8. El estándar 802.11*x* para la conectividad inalámbrica hace posible la instalación de una red *ad hoc* alrededor de una mesa de conferencia.

Es el tercer requisito el que llevó al IEEE a incluir como la frecuencia predilecta la de 2.4 GHz. Es una banda de frecuencia sin licencia que está reservada para usarse en el campo industrial, científico y médico de manera global.

Cómo funciona La red LAN 802.11 está basada en una arquitectura similar al diseño de redes de telefonía celular. Mediante el uso de un diseño de red similar, las redes inalámbricas pueden ofrecer los mismos beneficios de la telefonía celular, mientras que proporcionan velocidades más elevadas.

- **Celdas y grupos** Una LAN 802.11 se subdivide en celdas, y a cada celda se le conoce como un grupo de Basic Service Set (BSS, conjunto de servicio básico), que es el área de cobertura de un AP. Cada BSS está controlado por un punto de acceso. Pero, puesto que es posible que un solo punto de acceso no pueda satisfacer las necesidades inalámbricas de la red, se pueden conectar varios puntos de acceso a una espina dorsal común. Cuando se utiliza una configuración con varios puntos de acceso, se llama *sistema de distribución*. Sin importar qué tan grande o pequeña sea la red, ni cuántos nodos tenga conectados, el agrupamiento de equipo inalámbrico se puede ver como una sola red IEEE 802.11 por las capas superiores del Modelo de Referencia OSI. En la terminología 802.11, a las capas superiores del Modelo de Referencia OSI se les conoce como grupo de servicios extendido.
- **La capa física** El protocolo 802.11 abarca el control de acceso al medio y la capa física. Pero en lugar de un solo tipo de medio, el 802.11 soporta cuatro tipos: espectro extendido de saltos de frecuencia, espectro extendido de saltos de secuencia directa, el orthogonal frequency division multiplexing (OFDM, multiplexaje

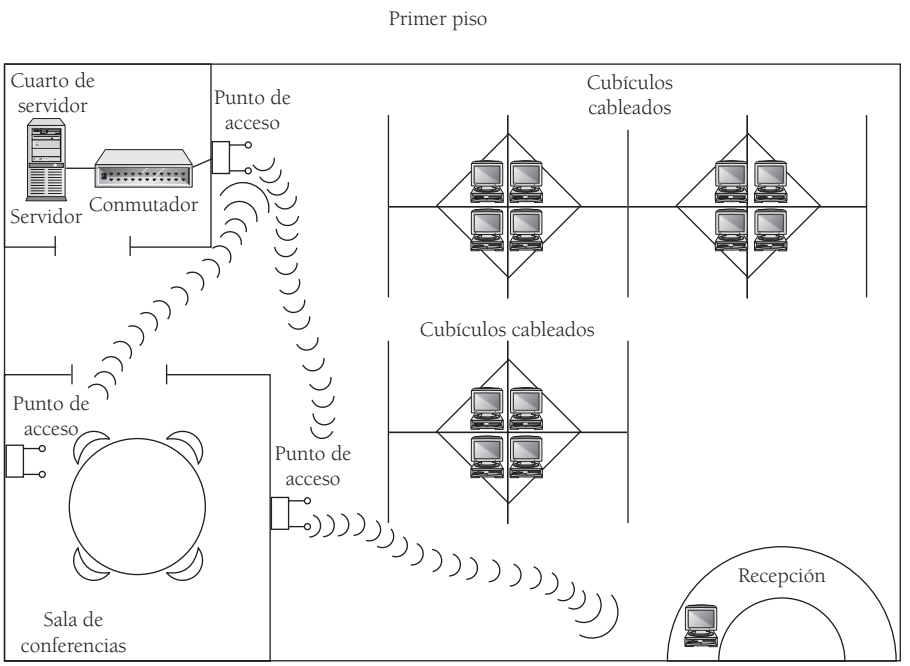


Figura 8-9. En este ejemplo, la distribución del primer piso de una compañía muestra cómo se pueden emplear los puntos de acceso.

ortogonal por división de frecuencia) y el infrarrojo. Una sola capa MAC soporta las tres capas físicas. Además, la capa MAC proporciona un vínculo con los protocolos de las capas superiores. Dentro de estas funciones se encuentra la fragmentación, la retransmisión de paquetes y los reconocimientos.

Como la arquitectura celular es la base de la conectividad inalámbrica, los dispositivos inalámbricos pueden conectarse, abandonar o circular de celda a celda de forma muy similar a como lo hacen los teléfonos celulares. El corazón de cada celda es un AP.

Establecimiento de la conexión Se utilizan dos métodos cuando se trata de conectarse realmente a un punto de acceso o a otra computadora. El primero tiene que ver con una estación que se conecte a una celda existente; el segundo incluye el proceso de moverse de una celda a otra:

- **Conexión a una celda existente** Hay tres momentos diferentes en que un dispositivo inalámbrico trata de acceder a un punto de acceso existente o a otro dispositivo inalámbrico: cuando el dispositivo se enciende, después de salir de un modo de reposo o cuando ingresa a una nueva área. En cada una de estas situaciones, el dispositivo necesita obtener información de sincronización. El dispositivo ubicará

a otro dispositivo para sincronizarse mediante el escaneo pasivo o activo. Pero, ¿cómo sabe un dispositivo que existen otros dispositivos inalámbricos con los cuales interconectarse? Con dos métodos diferentes de escaneo:

- **Escaneo activo** Este tipo de escaneo requiere que el dispositivo intente localizar un punto de acceso que pueda recibir información de sincronización de ese dispositivo. Esto se logra transmitiendo marcos de prueba y esperando un paquete de respuesta, transmitido por un punto de acceso.
- **Escaneo pasivo** Los dispositivos pueden escuchar un marco de señalización que se transmite periódicamente desde cada punto de acceso. El marco contiene información de sincronización, por lo que un dispositivo puede utilizarla para efectos de sincronización.
  1. Después de que un dispositivo ubica un punto de acceso y recolecta información de sincronización, éste intercambia información de autentificación. Los dispositivos y puntos de acceso intercambian una clave compartida, asegurando de este modo que uno tenga el derecho a hablar con el otro.
  2. Una vez que un dispositivo ha sido autentificado, las dos máquinas comienzan el proceso de asociación. Bajo este proceso, se analiza la información acerca del dispositivo y de las capacidades de los puntos de acceso disponibles. Se determina la ubicación actual del dispositivo y se asigna el mejor punto de acceso al dispositivo. Como es natural, si sólo hay un punto de acceso, el proceso de asociación es un hecho.

▲ **Roaming** En el último escenario, el dispositivo estaba conectado al punto de acceso y no era probable que se moviese. Se realizaba la conexión y el dispositivo estaba asociado con ese punto de acceso hasta que el usuario salía del sistema. Sin embargo, si se encuentra en un escenario en que un dispositivo se mueve de una celda (punto de acceso u otro dispositivo inalámbrico) a otra, a esa situación se le llama *roaming*. En la figura 8-10 se muestra este proceso.

Aunque es muy similar al roaming en un teléfono celular, existen dos diferencias importantes entre las tecnologías. La primera, la 802.11 soporta la transmisión de paquetes que cuentan con una dirección de destino específica, una secuencia y una identificación de fragmentos. Esto facilita el roaming en la LAN porque la transición entre celdas es a una velocidad más baja (caminar en comparación con manejar en un carro en un ambiente telefónico celular).

A continuación, si se presenta una breve interrupción en el servicio, ésta no causa tanto daño a una conversación telefónica como en un ambiente WLAN. Lo anterior se debe a que con una WLAN, una vez que se envían los paquetes, un protocolo de las capas superiores establece un tiempo antes de cada transmisión. Si el tiempo se acaba sin que la estación transmisora reciba un reconocimiento, volverá a enviar los paquetes. Por el contrario, en una red de telefonía celular, si se presenta una interrupción en la llamada, simplemente se pierde la voz y no hay un esfuerzo mecánico para reenviarlo. Sin embargo, en una WLAN, las interrupciones pueden significar tiempos más lentos debido a las retransmisiones.

Las celdas saben que ocurrirá el roaming, porque a medida que se aleja el dispositivo de un punto de acceso, dicho dispositivo podrá experimentar que la señal se hace cada vez más débil. El dispositivo utilizará su función de escaneo para tratar de encontrar un punto de acceso con una señal más fuerte. Una vez que se encuentre un nuevo punto de acceso, el dispositivo enviará una solicitud de reasociación. Luego, el nuevo punto de acceso enviará

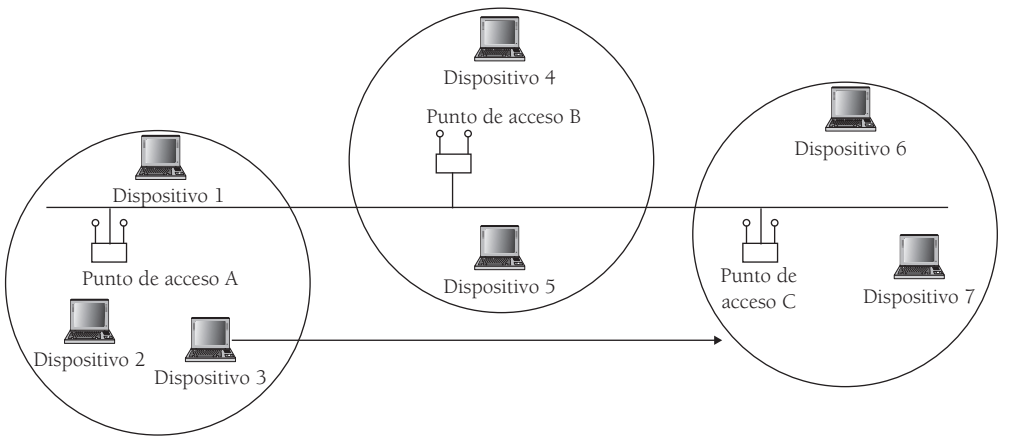


Figura 8-10. El roaming con un dispositivo inalámbrico significa que se mueve de una celda a otra.

un mensaje al punto de acceso del primer dispositivo para informar esta nueva asociación. Si el dispositivo no recibe una respuesta a la solicitud, buscará un nuevo punto de acceso.

Seguridad

Por mucho tiempo, el método estándar de seguridad utilizado para la conectividad inalámbrica fue la opción Wired Equivalent Privacy (WEP, privacidad equivalente a la cableada) del estándar 802.11. Los fabricantes soportan longitudes de clave de 128 bits. A medida que el tamaño de la clave es mayor, mejor será el nivel de seguridad. Sin embargo, en el año 2001 se vio que una persona puede violar la codificación WEP capturando millones de paquetes y operándolos a través de un número más pequeño de herramientas disponibles para la tarea. Después, en el 2004 se diseñó un nuevo método que permitía violar una codificación WEP con algunos miles de paquetes WEP capturados. En la actualidad, existen tantas herramientas para violar la codificación WEP, que ésta ya no se considera segura.

NOTA A pesar de que reconocemos que un gran número de puntos de acceso y estaciones de trabajo instaladas sólo soportan WEP, para efectos de seguridad, es recomendable que haga todo lo posible por usar WPA.

El Wi-Fi Protected Access (WPA, acceso protegido Wi-Fi) que se presentó en el 2003, puede utilizarse con un servidor de autentificación 802.1*x*. En una instalación típica, el servidor distribuye una clave de codificación diferente a cada usuario autenticado. También puede configurarse en un modo Preshared Key (PSK, llave precompartida), similar a la WEP, porque cada usuario utiliza la misma frase de acceso.

Tanto el WPA como el WPA2 están diseñadas para utilizar la autentificación 802.1*x*. Además del cifrado, ésta proporciona un medio más robusto de seguridad que la WEP. Mientras que la WEP se utiliza para cifrar datos, el cifrado WPA con la 802.1*x* se utiliza para permitir o negar que un cliente acceda a la red.

Precio

Los precios han caído significativamente en años recientes, y no hay un indicio de que vaya a haber algún cambio. El ahorro en cuanto al costo son circulares por naturaleza (a medida que la demanda de tecnología aumenta, es más barata la fabricación de unidades). Esto, a su vez, atrae a más clientes a la tecnología inalámbrica, lo que aumenta la demanda, lo que hace que sea más barata su fabricación, y así sucesivamente. No es muy probable que el precio del equipo para la conectividad inalámbrica sea alguna vez menor al correspondiente al equipo para cableado convencional. Sin embargo, una vez que se incluye el precio del cable y la mano de obra del cableado, los precios de las dos tecnologías son muy competitivos.

CONECTIVIDAD INALÁMBRICA DE CISCO

Cisco no logró ser el gigante de la interconectividad que es sentándose y esperando a que la buena suerte le cayera del cielo. En cambio, ha dado los pasos necesarios para posicionarse como líder en la tecnología de la conectividad. Algunas de sus inversiones e investigaciones han valido la pena, mientras que otras inversiones se han convertido en lecciones costosas para el grupo de desarrollo.

En esta sección, veremos cómo Cisco ha abarcado a la tecnología inalámbrica y la ha convertido en la tecnología del nuevo milenio. Después, hablaremos acerca de algunos de los productos para redes inalámbricas que Cisco ofrece.

Filosofía

No es de sorprenderse que Cisco no sólo haya abarcado la tecnología de redes inalámbricas, sino que también es líder en ese campo. Las recientes adquisiciones de Cisco se han hecho muy oportunamente, porque el mercado de las WLAN es cada vez más fuerte y la demanda, por parte de los usuarios, de acceso de alta velocidad a las redes corporativas es mayor que nunca.

Naturalmente, parte de esta bonanza en el mercado se debe al propio comportamiento de Cisco. En marzo del 2000, Cisco compró al fabricante de LAN inalámbricas Aironet Wireless Communications en 799 millones de dólares. En febrero de 1999, Cisco y Motorola anunciaron una sociedad de mil millones de dólares para desarrollar una infraestructura para redes inalámbricas basadas en Internet. Para consolidar las normas sobre las que operan las redes inalámbricas, en octubre de 1999 Cisco formó una sociedad con diez compañías enormes para diseñar estándares para los servicios de Internet inalámbricos de banda ancha. En noviembre de ese año, Cisco presentó sus primeros productos basados en esos estándares.

Cisco sigue ensanchando su mercado inalámbrico comprando cada vez más empresas. En 2003, Cisco compró Linksys Group en 500 millones de dólares. Esta adquisición significó para Cisco más clientes del mercado pequeña oficina/oficina en casa/consumidor. Se esperaba que las redes inalámbricas caseras crecieran de 2.7 miles de millones de dólares en el 2002 y hasta 7.5 miles de millones de dólares en el 2006.

Después, en 2005, Cisco compró Airespace, Inc. en 450 millones de dólares. Esto permitió a Cisco tener aún más clientes potenciales en el negocio inalámbrico mediante los puntos de acceso, las herramientas de administración y el software de Airespace. El equipo de Airespace permite una configuración centralizada y la administración de varios puntos de acceso.

Para Cisco, una compañía que hizo su fortuna y dominó el mercado del cableado, la transición a la tecnología inalámbrica representa un paso natural (además de ser una forma de mantener su participación en las áreas en desarrollo).

Productos de Cisco

Tomando en cuenta todas sus adquisiciones, Cisco puede ofrecer gran número de líneas de producto que sirvan a diferentes tipos de clientes de negocios, así como a usuarios caseros a través de su unidad Linksys. Pongamos especial atención aquí a los productos de negocios de Cisco.

Puntos de acceso

Comencemos con la línea de puntos de acceso de Cisco. En el centro de su línea de productos de puntos de acceso se encuentran los dispositivos de Aironet, pero su adquisición de Airespace ha agregado un par de modelos adicionales a la mezcla. Cisco ofrece puntos de acceso en todos los tamaños y medidas. Por ejemplo, puede conseguir un punto de acceso que maneje conexiones 802.11b/g, pero también hay puntos de acceso que trabajan en modo triple (es decir, los puntos de acceso como el Aironet 1130AG incluyen dos radios que pueden comunicarse con dispositivos 802.11b/g y 802.11a).

En la tabla 8-2 se comparan diferentes puntos de acceso de Cisco.

Controladores WLAN

En la tabla 8-2, el primer producto en la lista es el Cisco Lightweight AP de la serie 1000 . Esta línea de puntos de acceso proviene de la compra de Airespace. Están diseñados para utilizarse fácilmente en una organización y, por tanto, controlarlos con un controlador WLAN. Mientras que un punto de acceso como el 1240AG incluye en su interior información de la configuración, los puntos de acceso delgados dependen de la información de configuración enviada desde un controlador WLAN.

Estos controladores son el centro de la operación LAN inalámbrica. Son los dispositivos en que se almacenan la información de configuración y control, y después se envía a los puntos de acceso delgados.

	Cisco Light-weight Serie 1000 AP	**Aironet 1100**	**Aironet 1130AG**	**Aironet 1200**	**Aironet 1240AG**	**Aironet 1300**	**Aironet 1500 Light-weight Outdoor Mesh AP**
Estándar de red	802.11 a/b/g	802.11 b/g	802.11 a/b/g	802.11 a/b/g	802.11 a/b/g	802.11 b/g	802.11 a/b/g

Tabla 8-2. Línea de puntos de acceso de Cisco (*continúa*).

	Cisco Light-weight Serie 1000 AP	Aironet 1100	Aironet 1130AG	Aironet 1200	Aironet 1240AG	Aironet 1300	Aironet 1500 Light-weight Outdoor Mesh AP
Velocidad	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Rango	802.11a interiores: hasta 165 pies (50 m)	802.11b interiores: hasta 410 pies (124 m)	802.11a interiores: hasta 325 pies (100 m)	802.11g interiores: hasta 410 pies (125 m)	802.11g interiores: hasta 460 pies (140 m)	Con antena integrada	Depende del tipo de antena conectada
	Exteriores: hasta 1 000 pies (305 m)	Exteriores: hasta 700 pies (213 m)	Exteriores: hasta 650 pies (198 m)	Exteriores: hasta 700 pies (213 m)	Exteriores: hasta 950 pies (290 m)	hasta 1 410 pies (430 m)	
	802.11b en interiores: hasta 410 pies (124 m)	802.11g en interiores: hasta 410 pies (125 m)	802.11g en interiores: hasta 450 pies (137 m)	802.11a en interiores: hasta 500 pies (152 m)	802.11a en interiores: hasta 330 pies (100 m)	Con antenas opcionales, hasta 3 465 pies (1 055 m)	
	Exteriores: hasta 2 000 pies (610 m)	Exteriores: hasta 700 pies (213 m)	Exteriores: hasta 950 pies (290 m)	Exteriores: hasta 950 pies (290 m)	Exteriores: hasta 650 pies (198 m)		

Tabla 8-2. Línea de puntos de acceso de Cisco (*continúa*).

	Cisco Light-weight Serie 1000 AP	Aironet 1100	Aironet 1130AG	Aironet 1200	Aironet 1240AG	Aironet 1300	Aironet 1500 Light-weight Outdoor Mesh AP
	802.11g interio-res: hasta 300 pies (91 m) Exterio-res: hasta 1 300 pies (396 m)						
Seguri-dad	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP	802.11i, WPA2, WPA, 802.1X, AES, TKIP
Canales	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:	América: 11 China: 13 ETSI: 13 Japón: 13 (OFDM) 14 (CCK) Norte-américa: 11	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:	Banda de 2.4 GHz: América: 11 China: 13 ETSI: 13 Japón: (OFDM) 13, (CCK) 14 Norte-américa: 11 5 GHz band:

Tabla 8-2. Línea de puntos de acceso de Cisco (*continúa*).

Cisco Light-weight Serie 1000 AP	Aironet 1100	Aironet 1130AG	Aironet 1200	Aironet 1240AG	Aironet 1300	Aironet 1500 Light-weight Outdoor Mesh AP
América: 12		América: 12	América: 12	América: 12	América: 12	América: 12
China: 4		China: 4	China: 4	China: 4	China: 4	China: 4
ETSI: 9		ETSI: 9	ETSI: 9	ETSI: 9	ETSI: 9	ETSI: 9
Japón: 4		Japón: 4	Japón: 4	Japón: 4	Japón: 4	Japón: 4
Norte-américa: 12		Norte-américa: 12	Norte-américa: 12	Norte-américa: 12	Norte-américa: 12	Norte-américa: 12

Tabla 8-2. Línea de puntos de acceso de Cisco (*conclusión*).

Los controladores WLAN conservan información como:

- ▼ Directivas de seguridad.
- ■ Prevención de intrusiones.
- ■ Administración de radio-frecuencia (RF).
- ■ QoS (Quality of Service, calidad de servicio).
- ■ Movilidad.
- ▲ Configuración de puntos de acceso.

Pero los controladores WLAN no sólo administran información de la configuración; también responden a los cambios de entorno y uso para conservar la conectividad inalámbrica y la utilización de la red en un valor alto. Los controladores WLAN permiten:

- ▼ Asignación dinámica de canales para reducir la interferencia.
- ■ Detección de interferencia, seguido por la optimización de la red para reducir interferencia.
- ■ Equilibrio automático de cargas.
- ■ Cobertura de huecos detectados y corregidos.
- ▲ Ajuste automático de potencia a puntos de acceso específicos de la red.

Cisco ofrece dos series de controladores LAN inalámbricos:

- ▼ El Wireless LAN Controller (controlador LAN inalámbrico) de la serie 2000 está diseñado para aplicaciones empresariales de pequeño a mediano tamaño. Su modelo AIR-WLC2006-K9 puede controlar hasta seis puntos de acceso delgados.
- ▲ El Wireless LAN Controller de la serie 4400 está diseñado para empresas de tamaño mediano a grande. Tiene dos modelos: el 4402 y el 4404. El 4402 soporta 12, 25 o 50 puntos de acceso, mientras que el 4404 soporta 100.

Puentes inalámbricos Aironet de Cisco

Los puentes inalámbricos se utilizan para conectar dos o más redes ubicadas en lugares diferentes. Por ejemplo, los puentes pueden instalarse en varias escuelas de un distrito escolar y después utilizarse para conectar la LAN de cada escuela a una red más grande. Otra aplicación puede ser entre los diferentes pisos de un edificio en que simplemente es difícil instalar cable. El beneficio de un puente inalámbrico es que se alcanzan velocidades mayores a T1, pero las organizaciones no necesitan pagar líneas privadas o instalar fibras ópticas.

Cisco ofrece dos modelos de puentes inalámbricos, las series 1300 y 1400.

Puente inalámbrico 1300 Aironet de Cisco El Cisco Aironet 1300 Wireless Bridge es lo mismo que un punto de acceso de la serie 1300. Sin embargo, el producto hace una doble función, sirviendo como puntos de acceso y puente. Agregando diferentes tipos de antenas, un punto de acceso puede convertirse en puente.

Puente inalámbrico 1400 Aironet de Cisco El Cisco Aironet 1400 Wireless Bridge ofrece conectividad en campus, en Metropolitan Area Networks (MAN, redes de área metropolitana) y en cualquier situación en que sea necesaria la conectividad inalámbrica entre varios edificios o en edificios donde sea muy difícil instalar cableado.

Como en otros dispositivos 802.11a, la compensación entre altas velocidades y operación en la banda de 5 GHz es un rango mucho más pequeño que despliegues del 802.11b/g. Aironet 1400 Wireless Bridge trabaja a velocidades de hasta 54 Mbps y puede instalarse en vínculos punto a punto de hasta 35 kilómetros y en conexiones punto a multipunto de hasta 18 kilómetros. Dicho rango puede extenderse utilizando antenas de alta ganancia y disminuyendo las velocidades de transferencia de datos.

El puente también ofrece características avanzadas, como QoS y troncales de hasta 24 circuitos de Voice over IP (VoIP, voz sobre IP).

Adaptadores de cliente

La línea Aironet de Cisco ofrece tres diferentes tipos de adaptadores de cliente: la serie 350 de Aironet, el adaptador Wireless LAN Aironet de Cisco (para las distintas versiones de PCI y CardBus) y un adaptador 802.11a a 5 GHz. Los tres adaptadores utilizan cifrado de 128 bits para proporcionar seguridad.

Los adaptadores 350 de Aironet ofrecen hasta 11 Mbps de ancho de banda y un rango de hasta 450 metros. A medida que se encuentre más alejado del punto de acceso, su conexión será más lenta.

Del tipo de adaptador de cliente que tenga dependerá el tipo de computadora que puede tener. Las laptops y otras computadoras con una ranura PCMCIA utilizarán el PC Card Client Adapter (adaptador de cliente de tarjeta PC), mientras que los modelos de escritorio y torre utilizarán el PCI/ISA Client Adapter.

En la tabla 8-3 se proporciona una comparación entre estos adaptadores.

CONFIGURACIÓN DE LOS PUNTOS DE ACCESO

Hasta este punto, hemos hablado de los fundamentos de la tecnología inalámbrica, conceptos, posicionamiento de las compañías y la gran cantidad de productos que Cisco ofrece. Sin

	Cisco Aironet 350	Cisco Aironet CardBus Wireless LAN Adapter	Cisco Aironet PCI Wireless LAN Adapter	Cisco Aironet 5 GHz 54 Mbps 802.11a Wireless LAN Client Adapter
Estándar de red	802.11b	802.11 a/b/g	802.11 a/b/g	802.11a
Factor de forma	CardBus Tipo II o PCI	CardBus Tipo II	PCI	CardBus Tipo II
Rango	Hasta 2 000 pies (610 m)	Hasta 2 000 pies (610 m)	Hasta 2 000 pies (610 m)	Hasta 1 200 pies (355 m)
Velocidad	1, 2, 5.5 y 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Seguridad	WEP, TKIP y 802-1X	WEP, TKIP, WPA, 802.11i y 802-1X	WEP, TKIP, WPA, 802.11i y 802-1X	WEP, TKIP, WPA, 802.11i y 802-1X

Tabla 8-3. Línea de adaptadores de cliente inalámbrico de Cisco.

embargo, en esta sección, se tomará un enfoque más práctico e instalaremos y configuraremos una WLAN.

Por lo general, la instalación de un conmutador o enrutador significa encontrar un espacio en el cuarto del servidor, colocar el dispositivo en el lugar que corresponda y conectar el cableado. De alguna forma es un poco diferente con los puntos de acceso.

Como se observa, existen dos tipos básicos de equipo en una red inalámbrica: el puntos de acceso y un adaptador inalámbrico. El adaptador inalámbrico (del que hablaremos en algunas páginas más) es el componente móvil. Es el que puede conectar a una laptop y con el que se puede moverse por toda la compañía. Esa pieza de hardware puede moverse a cualquier lugar de su empresa siempre y cuando no se excedan los límites de distancia de los puntos de acceso.

Por el contrario, para contar con la flexibilidad de tener clientes móviles, puede ubicar el punto de acceso en un lugar óptimo.

Estudio del sitio

Muchas organizaciones acostumbran hacer estudios del sitio. Es un ejercicio en que un punto de acceso se coloca de manera temporal y se lleva un analizador de ancho de banda por todas las instalaciones para encontrar los mejores y peores puntos de conectividad. Los analizadores de ancho de banda son costosos, y si desea hacer este estudio, por lo general tendrá que conseguir un analizador rentado. Sin embargo, puesto que se necesita invertir un poco de tiempo para aprender a utilizar dicho aparato, es mejor contratar a alguien que cuente con el analizador y además tenga experiencia para hacer el trabajo.

Una vez realizado dicho estudio, éste puede indicarle:

- Ubicación ideal de los puntos de acceso.
- Velocidades y tasas de error de las diferentes ubicaciones.
- Si la cantidad de puntos de acceso que está planeando utilizar es adecuado.
- El desempeño de aplicaciones de la WLAN.

Colocación del punto de acceso

Cuando lleve a cabo un estudio del sitio, el primer paso es colocar el punto de acceso. Para empezar, ubique el punto de acceso lo más cerca posible de su posición final. Esto le ayudará a resolver cualquier problema que pueda presentarse después de que el punto de acceso sea montado en su posición final.

En casi todos los ambientes de oficina, los puntos de acceso deben montarse a la altura del techo. En las bodegas y otros sitios con techos altos, es mejor montarlos de 4 a 8 metros de altura.

Sin embargo, a esta altura, es probable que no cuente con contactos eléctricos convenientemente ubicados. Por ello, éste es el momento adecuado para utilizar Power over Ethernet (PoE, alimentación por Ethernet). PoE se puede agregar a su red Cisco utilizando un inyector de alimentación, como un panel de parcheo de alimentación de línea, y éste también es parte de algunos conmutadores Cisco (como los Catalyst, por ejemplo). Como su nombre lo sugiere, entrega potencia al dispositivo de descarga utilizando el mismo cableado Ethernet usado para entregar datos. PoE es una gran opción cuando se conectan puntos de acceso colocados remotamente o cuando no existen tomas de corriente ubicadas en lugares apropiados.

No hay razón para que sus puntos de acceso tengan que estar ubicado en la esquina de un escritorio o fijado a la pared. Es probable que resulte estético y ventajoso colocar su punto de acceso dentro del techo falso. Puede colocar sus antenas fuera del techo para obtener una conectividad óptima, pero el punto de acceso puede estar dentro del techo. Si opta por un dispositivo localizado en el techo falso, debe seleccionar uno que esté diseñado para configuración de antena remota.

NOTA Verifique los reglamentos locales respecto a incendios. Tal vez necesite puntos de acceso y cableado para techo falso si van a colocarse sobre los plafones del techo.

Interferencia

Es importante tomar en cuenta la interferencia al ubicar su punto de acceso. Necesita conocer las fuentes de interferencia como fotocopiadoras, hornos de microondas, teléfonos inalámbricos y todo lo que trabaje a la misma frecuencia que su punto de acceso.

Sólo para hacer la vida más interesante, el estándar 802.11g trabaja en la banda de 2.4 MHz; es la misma banda en que operan otros dispositivos sin licencia. Como tales, si su oficina tiene teléfonos inalámbricos que trabajen en esta banda, es posible que experimenten algo de interferencia.

Además, puesto que el uso de WiFi se ha extendido, es probable que experimente problemas porque un vecino puede estar utilizando un dispositivo WiFi. Si éste es el caso, necesitará cambiar canales.

Decir que las redes 802.11g ofrecen 11 canales es de alguna forma engañoso. Con las redes 802.11g, es necesario quitar cinco canales completos de otro dispositivo para evitar interferencia. Por lo general, las redes 802.11g operan en los canales 1, 6 y 11. Las redes 802.11a, por otra parte, poseen más canales disponibles para escoger, por lo que tiene más opciones si un vecino está utilizando equipo 802.11a.

Después de que haya llevado a cabo un estudio del sitio, verifique sus tasas de error y conectividad. Si los resultados no son satisfactorios, coloque el punto de acceso en algún otro lugar y trate de nuevo. Esto puede representar un trabajo largo y tedioso, pero si lo aborda tomando en cuenta las posibles fuentes de interferencia y la ubicación ideal, podrá ubicar el mejor sitio para su punto de acceso con razonable rapidez.

Configuración inicial

Configurar un puntos de acceso parece un trabajo desmoralizante (después de todo, estamos mezclando la conectividad de computadoras con transceptores de radio, por lo que se están mezclando dos ciencias). La verdad sea dicha, puede hacer la conectividad inalámbrica tan compleja como quiera.

Los puntos de acceso Aironet le permiten ser muy específico con sus parámetros para las funciones de la red y las del transceptor de radio. Puede tener control del tamaño de los paquetes, la potencia de transmisión y gran número de parámetros adicionales. Estos detalles se administran a través de un gran número de subpáginas en la página de configuración de Aironet.

Sin embargo, por fortuna, Cisco ha fabricado puntos de acceso que no sólo tienen gran número de opciones, sino que también son fáciles de usar. Los puntos de acceso pueden configurarse con facilidad y administrarse en forma rutinaria utilizando dos páginas de configuración express.

En esta sección, estudiaremos esas páginas de configuración inicial. Sin embargo, si necesita un control más detallado y eficiente del punto de acceso, dichas páginas se encuentran un poco fuera del alcance de lo que estudiaremos aquí; encontrará más información sobre esos parámetros en el sitio Web de Cisco.

Configuración express

Se accede a la página Express Setup (configuración express) abriendo un navegador Web e ingresando la dirección IP de su PA. Cuando accede por primera vez a su puntos de acceso, podrá observar una página de estado como la que se muestra en la figura 8-11.

En nuestro ejemplo, estamos utilizando un punto de acceso 1130AG Aironet de Cisco. Esto nos dice cuántos clientes se encuentran asociados (conectados) al punto de acceso, la dirección IP de éste, el estado de sus interfaces de red, un registro de eventos, etcétera.

Para obtener la página Express Setup, haga clic sobre el lado izquierdo de esta pantalla. La página Express Setup resultante se muestra en la figura 8-12.

Esta página le permite administrar detalles como:

- Nombre del host.
- Cómo se obtiene la dirección IP del puntos de acceso, a través del Dynamic Host Configuration Protocol (DHCP, protocolo de configuración dinámica del host) o estadísticamente.
- La dirección IP del dispositivo.
- La máscara de subred IP.

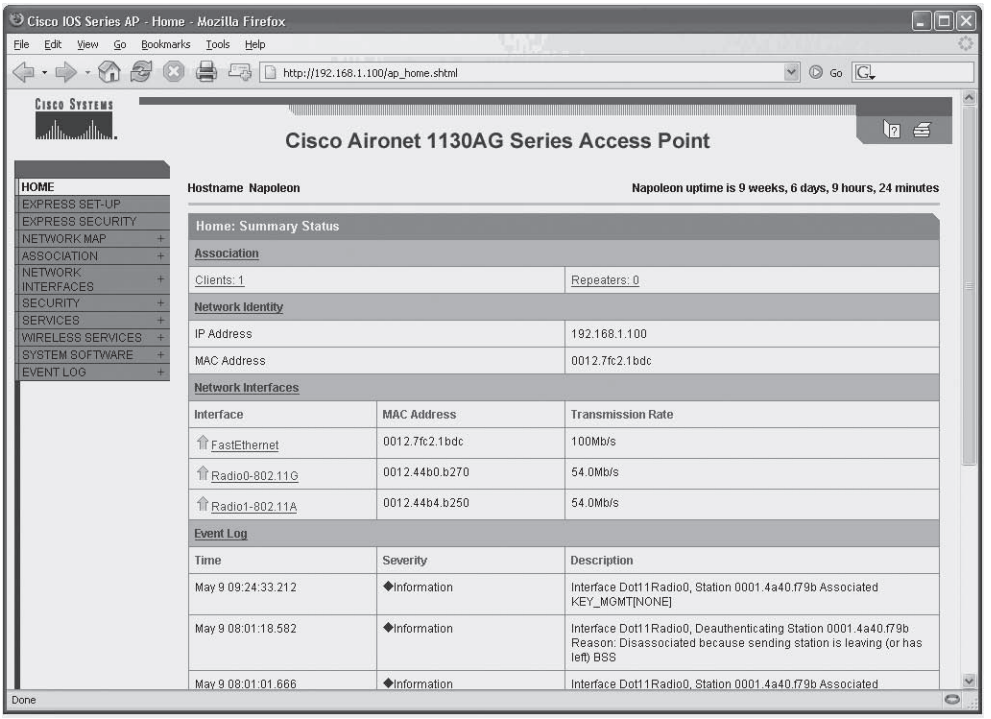


Figura 8-11. Una vez que ha accedido a un puntos de acceso de Cisco, la página de inicio le muestra un panorama de los parámetros del dispositivo.

- Gateway predeterminada.
- Comunidad SNMP.
- Si el punto de acceso es una raíz o un repetidor.
- Opciones para la optimización del desempeño de los puntos de acceso.
- Si las Aironet Extensions (extensiones de Aironet) están habilitadas o deshabilitadas. Habilitar las Aironet Extensions es lo ideal si su ambiente es totalmente Cisco.

NOTA Las Aironet Extensions proporcionan capacidades mejoradas cuando se utilizan otros dispositivos Aironet. Sin embargo, en entornos donde se utilizan otros productos inalámbricos, es mejor no habilitarlas.

Una vez que ha ingresado o configurado toda esta información, haga clic en el botón Apply ubicado en la esquina inferior derecha de esta página y se aplicarán los parámetros al punto de acceso.

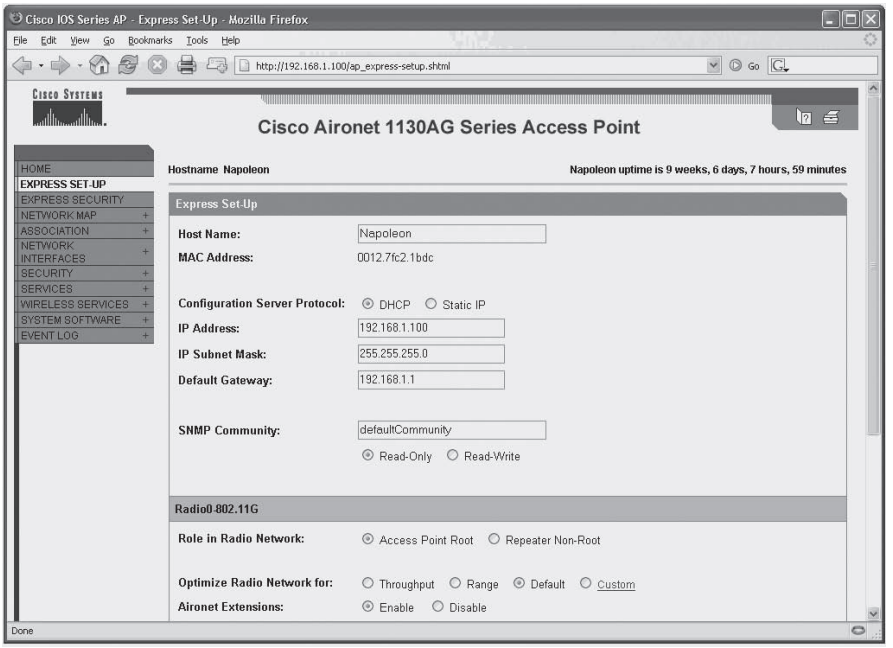


Figura 8-12. La página Express Setup del punto de acceso le permite administrar los parámetros más comunes de éste.

Express Security (seguridad express)

La seguridad es un aspecto tan importante en la conectividad en general y en la inalámbrica en particular, que Cisco ha dedicado una segunda página express a la administración de la seguridad de sus puntos de acceso. Ésta se administra a través de la página Express Security.

Al igual que en Express Setup, esta pantalla se utiliza para administrar de manera rápida y sencilla las funciones de la seguridad de su punto de acceso. Los detalles pueden administrarse con mayor profundidad desde cualquier otro punto del dispositivo, pero para efectos de la configuración inicial, éste es un lugar conveniente.

En la figura 8-13 se muestra esta página, a la que se accede a través de un vínculo en el lado izquierdo de las páginas de configuración del punto de acceso Aironet. Puede acceder a esta página desde cualquier lugar en la configuración de su punto de acceso haciendo clic en el vínculo que se encuentra a la izquierda.

Esta página le permite:

- Establecer sus Security Set Identifiers (SSID, identificadores para el conjunto de seguridad) del punto de acceso. Los SSID indican a qué parte de la red inalámbrica pertenece determinado punto de acceso.
- Habilitar y especificar las VLAN.

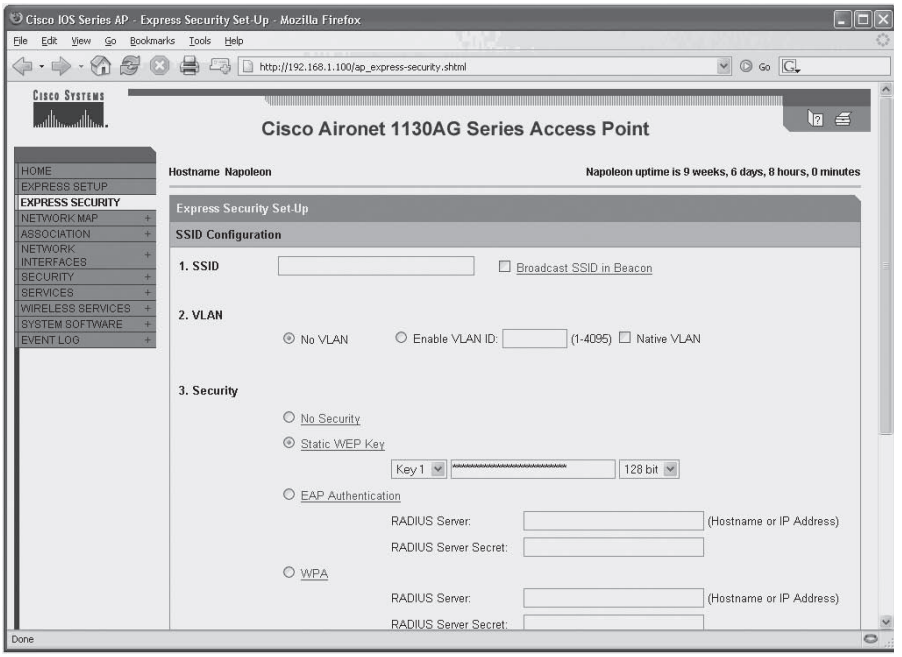


Figura 8-13. Una página de Express Security de un punto de acceso Aironet le permite la administración de los parámetros de seguridad.

- Configurar los protocolos de seguridad:
  - WEP (incluye la especificación de llaves WEP).
  - WPA.
  - 02.1X.
- ▲ Vista de una tabla que muestra los SSID de su puntos de acceso.

Esta página es una forma rápida de configurar las llaves WEP iniciales y de seleccionar entre las diferentes características que tendría que establecer en algún otro lugar dentro del archivo de configuración de su punto de acceso.

Hablemos acerca de cómo puede configurar y administrar las dos formas más comunes de claves WEP de seguridad del punto de acceso: WPA y 802.1x.

Seguridad

La medida de seguridad más sencilla y básica (y también la menos segura) de un punto de acceso es la clave WEP. Es una serie de caracteres alfanuméricos que se ingresan en el punto de acceso y en su cliente. Cuando un cliente trata de conectarse a un punto de acceso, debe contar con la clave correcta o no podrá conectarse. Aunque no debe ser su única forma de seguridad, al menos debe configurarse, en el caso de que no haya otras medidas de seguridad disponibles.

NOTA Las claves WEP son vulnerables y se pueden violar con facilidad. Dicho esto, habilitar la WEP es mejor que no hacer nada. Aunque no lo crea, muchas organizaciones no instalan ningún tipo de mecanismo de seguridad, ofreciendo una puerta abierta a su red. Es recomendable habilitar el WPA o el 802.1*x*. En caso de no poder hacerlo, al menos habilite WEP.

Claves WEP

Puede llevar a cabo tareas de claves WEP más detalladas mediante los pasos siguientes:

1. En el punto de acceso 1130AG de Aironet, haga clic sobre **Security**, en el lado izquierdo de la ventana.
2. Cuando la sección Security se expanda, haga clic en **Encryption Manager**. Esto despliega la pantalla que se muestra en la figura 8-14.
3. Esta pantalla le permite administrar la configuración de sus claves WEP:
   - ▼ **Encryption mode (modo de cifrado)** Contiene los parámetros para habilitar y deshabilitar la WEP, o establecer configuraciones de cifrado.
   - ■ **Encryption Keys (claves de cifrado)** Es la sección en la que se pueden ingresar hasta cuatro claves WEP y sus tamaños. Las claves WEP no se despliegan conforme las ingresa. Esto es una medida de seguridad, pero también hace que resulte difícil saber si ha tecleado erróneamente un carácter. Ingrese una clave en cada línea, si planea hacer una rotación de claves WEP.
   - ▲ **Global Properties (propiedades globales)** Se utilizan para administrar el comportamiento de sus claves WEP. Aquí puede seleccionar si hace una rotación de las claves, cuál es el intervalo entre cada giro y cómo se administrarán las claves dentro de su grupo.
4. Puesto que el punto de acceso 1130AG de Aironet tiene radios a 2.4 y 5 GHz, estos parámetros pueden aplicarse a cualquiera de los radios o a ambos. En este caso, hacer clic en **Apply-Radio0** podría establecer estos parámetros para el radio a 2.4 GHz. Si hace clic eb **Apply-All** enviará los parámetros a ambos radios.

WPA

Para responder a las deficiencias de WEP, la WiFi Alliance presentó en el 2003 WiFi Protected Access (WPA, acceso protegido WiFi).

WPA combina la autentificación (mediante el uso de un servidor de autentificación) y el cifrado para asegurar la conexión. WPA mejoró a WEP mediante el uso de claves de cifrado que cambian de manera automática, utilizando el Temporal Key Integrity Protocol (TKIP, protocolo de integración temporal de claves).

Existen dos versiones de WPA de las que tal vez haya escuchado: WPA y WPA2. Casi siempre, proporcionan la misma funcionalidad. La diferencia principal entre las dos es el método de cifrado. WPA utiliza un cifrador de ráfagas RC4, con una clave de 128 bits y un vector de inicialización de 48 bits. Cuando se utiliza un vector (mientras más grande, mejor) junto con el mecanismo de giro de clave del TKIP, se hace cada vez más difícil violar el cifrado del sistema.

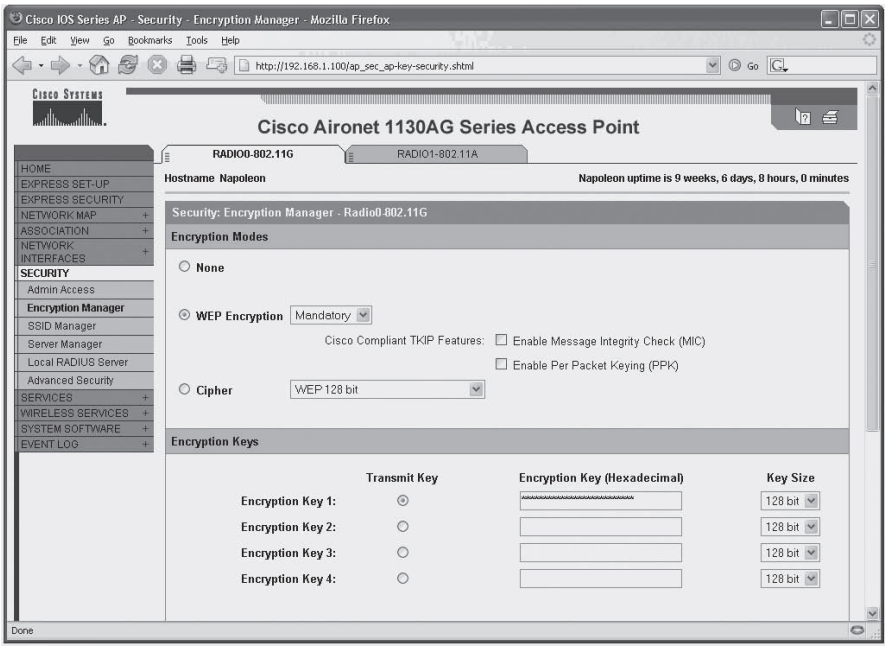


Figura 8-14. Encryption Manager se utiliza para configurar y administrar el cifrado de su punto de acceso.

WPA2 reemplaza a RD4 con AES, un método de cifrado más robusto. Si WPA2 se encuentra disponible en sus clientes y punto de acceso dependerá de la versión del firmware que esté utilizando.

NOTA WPA fue diseñado como una etapa intermedia para lograr la autentificación 802.1x. Una de las razones principales fue que el desarrollo y finalización del 802.1x tomó más tiempo del que se tenía previsto y, durante ese tiempo, las organizaciones se preocuparon cada vez más de las debilidades de la seguridad.

WPA también hizo que las transmisiones inalámbricas tuvieran más poder de adaptación. El sistema no sólo proporciona autentificación y cifrado, sino que también mejora la integridad de la información. La Cyclic Redundancy Check (CRC, verificación de redundancia cíclica) en WEP es insegura, y es posible modificar la información o actualizar el mensaje CRC sin conocer de antemano la clave WEP. WPA utiliza un Message Integrity Code (MIC, código para la integridad del mensaje). El MIC utilizado en WPA utiliza el contador de marcos, evitando los ataques repetidos, que representan otra debilidad de la WEP.

Demos un paseo por el proceso para configurar WPA en su punto de acceso. Sin embargo, antes de comenzar, suponemos que cuenta con una configuración de trabajo LEAP, EAP o PEAP.

Para comenzar, recorra el Encryption Manager de su punto de acceso. Estamos utilizando un punto de acceso Aironet 1130AG de Cisco. Estos pasos serán muy similares, sin importar qué puntos de acceso de Cisco esté utilizando, pero no se sorprenda si se encuentra con ligeras diferencias basadas en el modelo del punto de acceso que esté utilizando y la versión de firmware que esté operando.

Se accede a Encryption Manager, que se muestra en la figura 8-14, desde la página de inicio del punto de acceso seleccionando **Security | Encryption Manager**.

Desde aquí, siga estos pasos:

1. Seleccione la opción **Cipher**.
2. Selecciones **TKIP** del menú desplegable.
3. Quite la marca en **Encryption Key 1**.
4. Seleccione la opción **Transmit Key** que está junto a Encryption Key 2.

Los resultados de estos pasos se muestran en la figura 8-15.

5. Haga clic en la opción **Apply-Radio#** en la parte inferior de la página.
6. A continuación debe configurarse el SSID Manager. En el menú que se encuentra en el extremo izquierdo, seleccione **SSID Manager**.

El SSID Manager se muestra en la figura 8-16.

7. Seleccione el SSID deseado de la lista Current SSID List.
8. Con base en el tipo de clientes que se conectarán al punto de acceso, seleccione el método de autenticación que se utilizará. En la tabla 8-4 se proporciona una lista con los tipos de clientes y la selección que debe hacer.
9. En la opción Authenticated Key Management, seleccione **Mandatory** en el menú desplegable.
10. Marque la casilla de verificación **WPA**.
11. Haga clic en **Apply-Radio#** en la parte inferior de la página.

La configuración WPA puede verificarse seleccionando **Association** del menú que se encuentra hastíen el extremo izquierdo de la página de inicio de su punto de acceso, y después seleccionando la dirección MAC del cliente. Si el WPA se configuró adecuadamente, se desplegará el TKIP.

802.1x

WEP es rápida y sencilla, pero también puede ser violada por un hacker dedicado. La autentificación 802.1x proporciona un medio de seguridad más fuerte.

NOTA Para instalar la autentificación 802.1x, debe contar con un servidor RADIUS en su red.

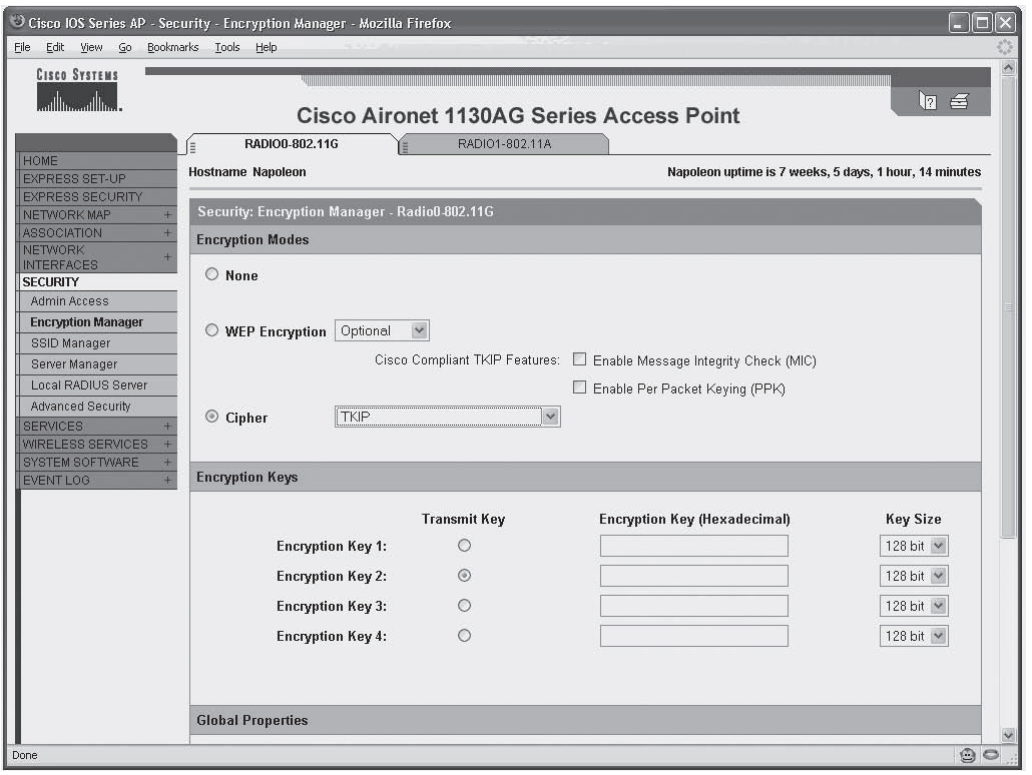


Figura 8-15. WPA se configura en la página Encryption Manager.

Para configurar la autentificación 802.1x, siga estos pasos:

1. Haga clic en **Express Security** en el menú que se encuentra a la izquierda de la pantalla de configuración del punto de acceso.
2. En Security, establezca si desea que no haya seguridad, una clave WEP estática (junto con un espacio para ingresar la clave), autentificación EAP o WPA.
3. Para configurar LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM y otros protocolos basados en 802.1x/EAP, haga clic en la opción relevante junto a EAP Authentication. Para usar WPA, haga clic en la opción **WPA Authentication**.
4. En los cuadros junto a EAP Authentication o WPA Authentication, ingrese el nombre del servidor RADIUS y el secreto que se compartirá entre el punto de acceso y el servidor RADIUS.
5. Haga clic en **Apply**.

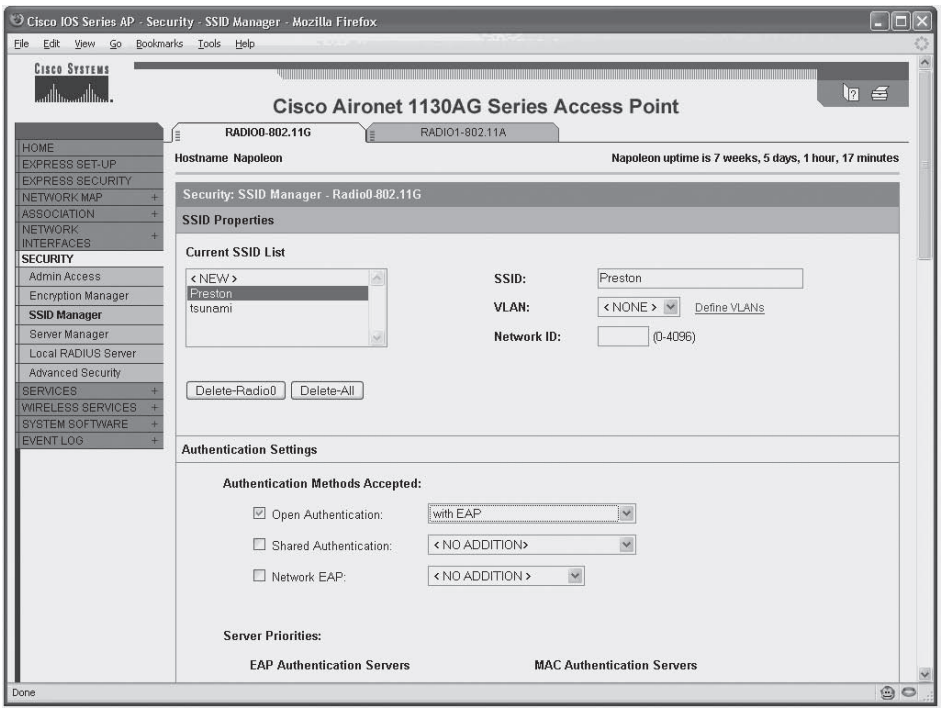


Figura 8-16. El SSID Manager puede configurarse seleccionándolo en el menú Security del lado izquierdo de la página.

Tipo de cliente	Método de autentificación
Clientes de Cisco.	Utiliza Network-EAP.
Clientes de terceros incluidos los clientes de Cisco Compatible Extension (CCX, extensión compatible de Cisco).	Utiliza Open Authentication (autentificación abierta) con EAP.
Clientes de Cisco y de terceros.	Utiliza el Network-EAP y la Open Authentication con EAP.

Tabla 8-4. Métodos de autentificación para los tipos de cliente.

Estos parámetros permiten una rápida configuración de la autentificación 802.1x. Para tener mayor control sobre el manejo de la 802.1x de su punto de acceso, haga clic en Security, en el menú que se encuentra a la izquierda. Lo anterior le permite hacer cosas como especificar los servidores RADIUS de respaldo, habilitar la contabilidad, administrar el puerto de autentificación y algunos detalles adicionales.

Colocación de las antenas

Existen dos tipos de puntos de acceso, uno que emplea antenas internas (como el Aironet 1130AG) y otro que utiliza antenas externas (como el Aironet 1240AG).

Los que requieren antenas externas no están diseñados de esa forma para provocar inconvenientes; más que eso, proporcionan un uso y un despliegue más flexibles. Es decir, hay algunas consideraciones importantes que se deben tener presentes cuando se conecta una antena externa a su punto de acceso: la antena debe estar ubicada lo más cerca posible al punto de acceso. A medida que la antena se encuentre más alejada de éste, se reduce más la señal. Por ejemplo, si está instalando antenas para cubrir un patio exterior, no coloque el punto de acceso en el gabinete del servidor que se encuentra dentro del edificio. En este caso, es mejor colocarlo fuera, en un contenedor a prueba de agua (o comprar un punto de acceso a prueba de agua desde el principio), para que esté más cerca de la antena.

El tipo de cableado de antena que utilice es un aspecto muy importante también. La pérdida de señal se verá afectada por el tipo de cable que use. Es de esperarse una pérdida de aproximadamente 6 dB por cada 30 metros de cable. Cuanto más grueso sea el cable, mejor. Sin embargo, el cable más grueso es más caro y difícil de instalar.

El tipo de punto de acceso inalámbrico que utilice también será un factor. Si está utilizando un punto de acceso 802.11a, la pérdida en el cable será más significativa a medida que aumenta la frecuencia. Por ello, debe esperar que una pérdida mayor entre antenas con un punto de acceso 802.11a que con uno 802.11g.

CONFIGURACIÓN DEL CLIENTE

Una vez que se ha configurado el punto de acceso, el siguiente paso es configurar sus clientes. Hay dos formas en que puede hacerlo: mediante el sistema operativo de una computadora (el Windows XP Service Pack 2, por ejemplo, tiene una soporte robusto para opciones inalámbricas) o mediante utilerías que Cisco incluye en sus adaptadores inalámbricos. En esta sección se explica cómo configurar su adaptador usando las utilerías de Cisco.

Cisco ofrece diferentes utilerías para el cliente. La Desktop Aironet Utility (ADU, utilería de escritorio de Aironet) se utiliza para las tarjetas PCI y 802.11a/b/g CardBus, mientras que la Aironet Client Utility (ACU, utilería de cliente de Aironet) se usa para otros adaptadores.

Instalación

La instalación de una tarjeta PC en una laptop es un proceso relativamente fácil (conéctela y está lista). Sin embargo, si está instalando una tarjeta inalámbrica en una PC de escritorio, los pasos que hay que seguir son un poco más complicados. Siga estos pasos para instalar un adaptador inalámbrico basado en una tarjeta PCI:

1. Apague la computadora, abra la cubierta y busque una ranura PCI que se encuentre disponible.
2. Deslice la antena por la apertura de la cubierta de la tarjeta PCI abierta.
3. Conecte la tarjeta PCI, asegurándose de que se encuentre firmemente asentada en su base.
4. Asegure la tarjeta con el tornillo de montaje y coloque de nuevo la cubierta del equipo.
5. Deslice la antena a través de su base de montaje y asegúrela.
6. Coloque la antena en algún lugar alejado de repisas de metal, hornos de microondas o cualquier otra fuente de interferencia. La base de la antena puede montarse sobre una pared si así lo prefiere.

Una vez que se ha instalado el hardware, se debe hacer lo mismo con el software. Cuando el cliente se inicialice, si ve el Asistente para nuevo hardware encontrado de Windows, haga clic en Cancelar, porque deberá instalar software de Cisco.

El CD que viene con el adaptador de cliente tendrá un asistente Install incluido; sin embargo, es mejor obtener el asistente del sitio Web de Cisco, para asegurarse de que cuenta con la última versión. Hasta el momento en que se escribió este libro, puede acceder a la página http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless. Esta página contiene software actualizado de todos los productos inalámbricos de Cisco. Sin embargo, esté alerta, porque necesitará una cuenta válida de conexión en línea de Cisco.

Para encontrar el software correcto para su adaptador, diríjase a la página Web que se mencionó antes y navegue por ella siguiendo estos pasos:

1. Expanda la opción **Wireless LAN Access**.
2. Haga clic en **Cisco Wireless LAN Client Adapters**.
3. Haga clic en el adaptador inalámbrico que esté utilizando. Se le solicitará una cuenta CCO en este punto.
4. Seleccione la plataforma que está utilizando (Windows 2000 o Windows XP).
5. Haga clic en el archivo Install Wizard que tenga el número de versión mayor.
6. Tendrá que llenar un formulario en línea y aceptar los términos del software, y después comenzará la descarga y podrá iniciar el asistente.
7. Una vez que ha descargado el software, instálelo siguiendo las instrucciones que aparecen en la pantalla.

Hay un paso importante durante la instalación para los usuarios de Windows XP que utilicen ADU. Al mismo tiempo que se instalen los controladores, se le preguntará si desea instalar ADU o una herramienta de terceros. Puede seleccionar la opción que desee, pero si elige administrar su adaptador con una herramienta de terceros, ADU no se instalará y tendrá que seguir las instrucciones de configuración del otro fabricante. Si instala ADU, se deshabilitará Microsoft Wireless Configuration Manager.

Configuración

Una vez que el hardware y el software se han instalado, el siguiente paso consiste en configurar su adaptador. Abra la aplicación ADU o ACU (dependiendo de la herramienta que tenga instalada) y haga clic en la ficha **Profile Management**.

NOTA Los pasos que se muestran aquí pueden diferir ligeramente en función de la versión de software que esté utilizando. Debido al gran número de variantes de software que se pueden tener, sería imposible incluirlas todas aquí, pero estos pasos deberán ayudarle a comprender los parámetros de su versión en particular.

El Profile Manager se utiliza para administrar diferentes perfiles para su cliente. Por ejemplo, si la computadora cliente está siendo utilizada por dos o más redes inalámbricas, el Profile Manager puede efectuar un conjunto discreto de configuraciones de cada red, y conectarse a una red diferente es tan fácil como seleccionar un nuevo perfil.

Cree un nuevo perfil

Para crear un nuevo perfil, siga estos pasos:

1. Haga clic en **Add**.
2. Ingrese un nombre para su nuevo perfil, y presione ENTER.
3. Cuando aparezca la pantalla Properties, utilice las propiedades especificadas en forma predeterminada o haga los cambios que desee a los parámetros del sistema.

Los parámetros del sistema que se muestran en la figura 8-17, le permiten establecer y administrar parámetros específicos de su perfil. En la tabla 8-5 se explican estos parámetros.

4. Una vez que se hayan ingresado los parámetros, haga clic en **OK** para regresar a la pantalla Profile Manager.
5. Para incluir este perfil en la selección auto profile, marque la casilla de verificación **Include Profile in Auto Profile Selection** en la pantalla del Profile Manager.
6. Haga clic sobre **OK**.

Selección del perfil

Después de haber creado sus perfiles, debe seleccionar el perfil que utilizará. Esto se lleva a cabo mediante los pasos siguientes:

1. Abra ACU o ADU y después seleccione **Select Profile** desde el menú desplegable de comandos. En la figura 8-18 se muestra la pantalla Select Profile.
2. Seleccione una de las opciones siguientes:
   - ▼ **Use Selected Profile** Utiliza el perfil específico que seleccionó. Si el adaptador no puede asociarse con un punto de acceso o pierde dicha asociación, no seleccionará automáticamente otro perfil para intentar una conexión.
   - ■ **Use Auto Profile Selection** El controlador del adaptador seleccionará de manera automática un perfil de la lista. Si no puede asociarse o pierde la asociación, después de 10 segundos, se cambiará a otro perfil (suponiendo que se ha configurado más de uno) y se tratará de reasociar.
   - ▲ **Use Another Applications To Configure My Wireless Settings** Esta opción permite que otras aplicaciones (como las que incluidas en Windows XP) configuren el adaptador del cliente.
3. Haga clic en **OK**.

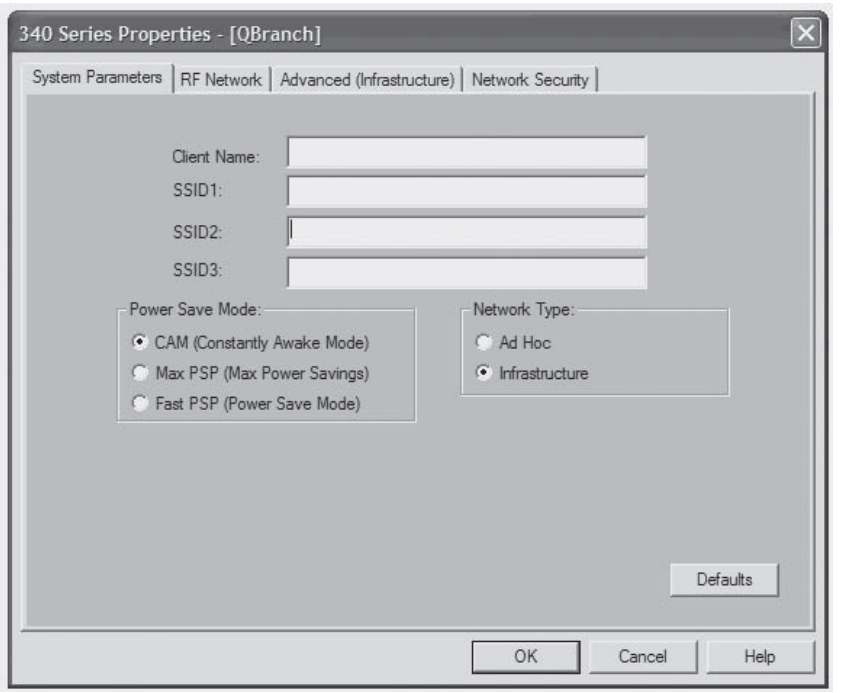


Figura 8-17. Los parámetros del sistema inalámbrico se administran fácilmente en el cliente.

Seguridad del cliente

La seguridad del cliente se administra utilizando la ficha Network Security. Esta pantalla se muestra en la figura 8-19.

Esta pantalla le permite administrar las claves WEP y los parámetros 802.1x. En esta sección, estudiaremos los fundamentos y la administración de las claves WEP.

NOTA El 802.1x es mucho más complejo y no se estudia aquí. Para obtener mayor información acerca de la administración de los parámetros del 802.1x, visite la página www.cisco.com.

Antes de efectuar algún cambio a los parámetros de seguridad del adaptador, tiene que decidir cómo configurar el parámetro Allow Associated To Mix Cells, ubicado en la parte inferior de la pantalla. Esto establece si el cliente puede asociarse con celdas utilizando las asociaciones WEP y no WEP.

Seleccione esta casilla de verificación si su punto de acceso tiene WEP en Optional y la WEP no está habilitada en el cliente. Quite la marca de esta casilla de verificación si el punto de acceso no tiene la opción WEP en Optional.

Parámetro	Descripción
Client Name	Proporciona un nombre para su cliente y le permite ser identificado en la red y en el punto de acceso.
SSID1	El Service Set Identifier (SSID, identificador de conjunto de servicio) indica a qué red inalámbrica desea tener acceso. El SSID es un identificador único, sensible a mayúsculas y minúsculas, que está conectado a paquetes seleccionados y enviados a través de la red inalámbrica. Los nodos asociados con el dispositivo deben utilizar el mismo SSID, o sus solicitudes de asociación serán ignoradas. Si el parámetro se deja en blanco, el cliente puede asociarse con cualquier punto de acceso que esté configurado para permitir la difusión amplia de las SSID.
SSID2	Es un SSID opcional que permite que el cliente rastree otra red sin que necesite reconfigurar el cliente.
Power Save Mode	Parámetros de ahorro de energía: ▼ **CAM (Constantly Awake Mode, modo para despertar constantemente)** El cliente es alimentado constantemente para obtener una respuesta máxima. Es el valor menos eficiente de energía y deja sin energía la batería de la laptop. ■ **Max PSP (Maximum Power Savings, máximos ahorros de energía)** El punto de acceso almacena los mensajes entrantes del cliente. El cliente "despierta" periódicamente para verificar el punto de acceso. Después, cualquier mensaje almacenado se envía al cliente. Este modo conserva la mayor cantidad de energía, pero ofrece la menor utilización del sistema. ■ **Fast PSP (PSP rápido)** Este modo alterna entre los modos PSP y CAM, en función al tráfico en la red.
Network Type	Especifica a qué tipo de red se conectará su adaptador: ■ ***Ad Hoc*** Se utiliza cuando la red inalámbrica se compone de dispositivos inalámbricos que no están conectados a una LAN alámbrica o inalámbrica. ▲ **Infraestructura** Se utiliza cuando se conecta a una red a través de un punto de acceso.

Tabla 8-5. Parámetros del sistema cliente inalámbrico.

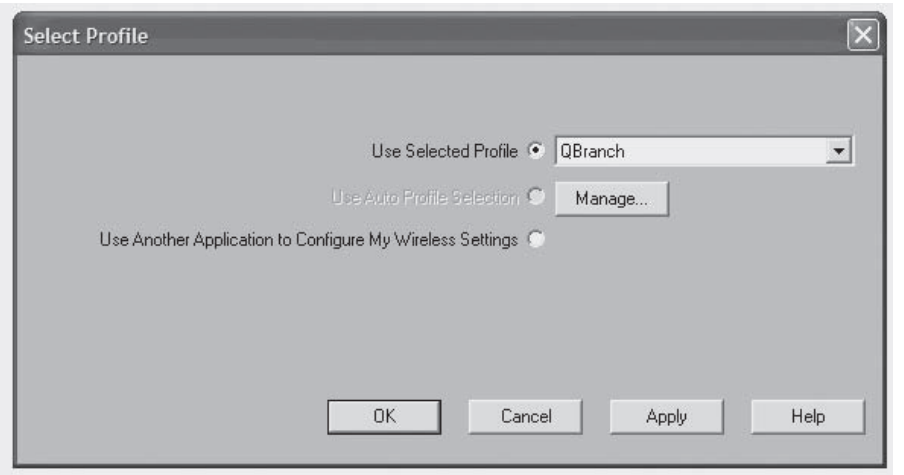


Figura 8-18. Necesita seleccionar el perfil que utilizará en su WLAN.

Configuración de claves WEP

Las claves WEP se pueden configurar para un cliente mediante los pasos siguientes:

1. Seleccione **None** del cuadro desplegable Network Security Type, en la pantalla Network Security.
2. Seleccione **Use Static WEP Keys**.
3. Elija uno de los formatos de claves WEP siguientes:
   - ▼ **Hexadecimal (0-9, A-F)** Las claves se ingresarán al sistema en formato hexadecimal: números 0-9 y letras A-F (en mayúsculas o minúsculas).
   - ▲ **ASCII Text** Las claves WEP se ingresarán con texto ASCII, incluidos caracteres, números y signos de puntuación.
4. Elija una opción de autentificación de puntos de acceso. Esto establece la forma en que su cliente se autentificará con el puntos de acceso:
   - ▼ **Open Authentication** Se permite al adaptador del cliente comunicarse con el punto de acceso, sin tomar en cuenta los parámetros WEP.

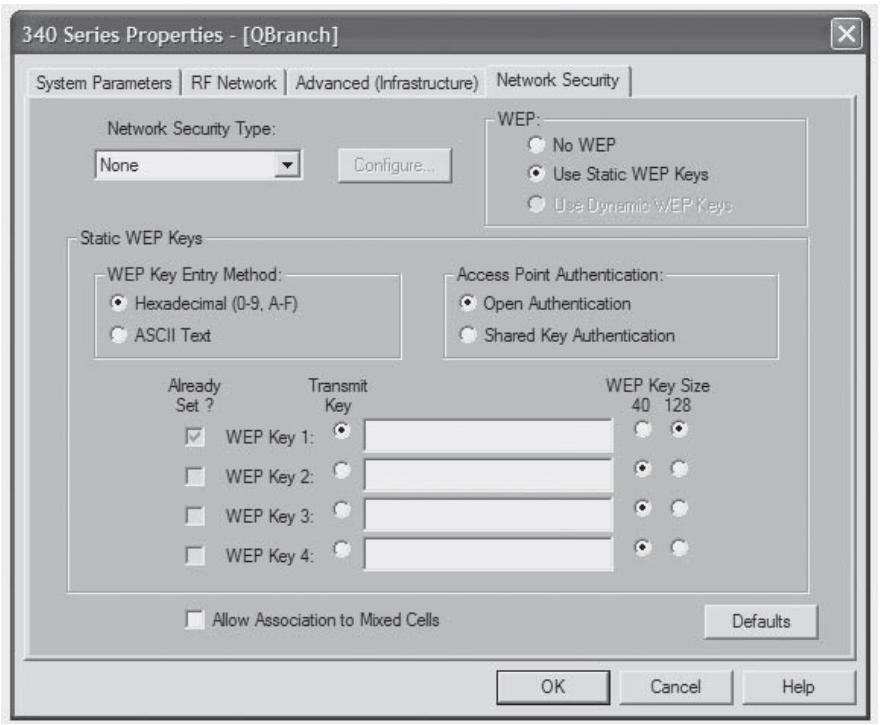


Figura 8-19. La seguridad del cliente se administra utilizando la ficha Network Security.

▲ **Shared Key Authentication** El adaptador del cliente sólo puede comunicarse con un punto de acceso que comparta la misma clave WEP.

5. Seleccione un tamaño de clave, de 40 o 128 bits. Los clientes con adaptadores de 128 bits pueden utilizar cualquier tamaño de clave, pero los clientes con adaptadores de 40 bits sólo pueden usar claves de 40 bits.
6. Teclee la clave WEP en el campo correspondiente. Una de las razones principales (si no es que es la principal) por la que los clientes no se configuran correctamente es por un error al teclear la clave WEP. Las claves WEP de 40 y 128 bits tienen diferentes tamaños:

   ▼ Las claves de 40 bits contienen diez caracteres hexadecimales (4A2b8DaA10, por ejemplo) o cinco caracteres de texto ASCII (por ejemplo, k@1D3).

   ▲ Las claves de 128 bits contienen 26 caracteres hexadecimales (123abc-456dEF123Abc321Cba78, por ejemplo) o 13 caracteres de texto en ASCII (por ejemplo, c@nN0nd@le4o0).

NOTA Sea cuidadoso con el uso de mayúsculas y minúsculas, y si se está usando "0" u "o".

7. Haga clic en la opción **Transmit Key** que se encuentra a la izquierda de la clave que desea utilizar para transmitir paquetes.
8. Haga clic en **OK** para regresar a la pantalla Profile Manager.
9. Haga clic en **OK** para guardar sus valores.

Configuración del 802.1x

Mientras que la configuración de WEP de un cliente inalámbrico es relativamente sencilla, el proceso se dificulta cuando se configura el 802.1x.

Puede configurar dos tipos de 802.1x en su adaptador inalámbrico de Cisco: el LEAP y el EAP basado en host.

NOTA Además de configurar el 802.1x en su adaptador inalámbrico, también se le solicitará habilitarlo en su sistema operativo. Los pasos que hay que seguir están fuera del alcance de lo que estamos haciendo aquí, por lo que deberá verificar con el fabricante de su sistema operativo para que le informe cómo habilitar cualquier versión del 802.1x que esté utilizando.

LEAP Para configurar la autenticación del LEAP en el dispositivo del cliente, siga estos pasos:

1. Seleccione **LEAP** en el cuadro desplegable Network Security Type.
2. Haga clic en **Configure**. Aparecerá una nueva pantalla con varios parámetros.
3. Habrá de seleccionar una opción de configuración de nombre de usuario y contraseña LEAP:
   - ▼ **Use Temporary User Name and Password** El adaptador requerirá de un nombre de usuario y una contraseña cada vez que reinicie la computadora para autentificarse en la red.
   - ▲ **Use Saved User Name and Password** El adaptador no requerirá de un nombre de usuario y una contraseña cada vez que la computadora se reinicie. La autentificación se presentará utilizando un nombre de usuario y una contraseña guardada.
4. Si selecciona Use Temporary User Name and Password en el paso 3, seleccione una de estas opciones (de lo contrario, vaya al paso 5):
   - ▼ **Use Windows User Name and Password** El nombre del usuario y la contraseña del cliente Windows son también los del LEAP. Ésta es la configuración predeterminada.
   - ■ **Automatically Prompt for LEAP User Name and Password** Se debe utilizar un nombre de usuario y una contraseña diferentes a las correspondientes del cliente Windows. Éstos se solicitan en el proceso para ingresar a Windows.
   - ▲ **Manually Prompt for LEAP User Name and Password** El cliente debe solicitar la autentificación LEAP.

5. Si selecciona Use Saved User Name and Password en el paso 3, siga estos pasos:
   - ▼ Ingrese un nombre de usuario y una contraseña.
   - ■ Reingrese la contraseña en el campo Confirm Password.
   - ▲ Si fuera necesario, teclee un nombre de dominio que será enviado al servidor RADIUS junto con el nombre de usuario del cliente, en el campo Domain.
6. Si está trabajando en un ambiente con varios dominios y desea que su dominio de inicio de sesión de Windows sea enviado al servidor RADIUS junto con su nombre de usuario, marque la casilla de verificación **Include Windows Login Domain With User Name**.
7. Para desasociar cuando el cliente se salga del sistema, marque la casilla de verificación **No Network Connection Unless User is Logged In**.
8. En el campo LEAP Authentication Timeout Value, teclee el número de segundos que el cliente tendrá que esperar antes de que la autentificación se considere una falla. Este valor varía entre 30 y 300 segundos.
9. Haga clic en **OK**.
10. Haga clic en **OK**.
11. Haga clic en **OK**.

EAP Basado en host Para habilitar EAP basado en host, siga estos pasos:

1. Seleccione **Host Based EAP** del menú desplegable Network Security Type, en la pantalla Network Security.
2. Dependiendo del tipo de EAP que planee utilizar, realice cualquiera de las acciones siguientes:
   - ▼ Si habrá de autentificar con EAP-TLS, PEAP o EAP-SIM, seleccione **Use Dynamic WEP Keys** bajo la WEP.
   - ■ Si habrá de autentificar con EAP-MD5 con WEP estática, seleccione **Use Static WEP Keys** y después ingrese una clave WEP estática.
   - ▲ Si utiliza EAP-MD5 sin WEP, seleccione **No WEP** bajo la WEP.
3. Haga clic en **OK**.
4. Haga clic en **OK**.

La conectividad inalámbrica se encuentra todavía en una etapa muy joven de desarrollo. A pesar de que son factibles logros importantes, espere más de Cisco y de la comunidad inalámbrica en los próximos años.

PARTE III

Soluciones de negocios de Cisco

CAPÍTULO 9

Centro de contacto unificado de Cisco

En el centro de la oferta de Cisco se encuentran sus populares enrutadores, conmutadores y servidores. Éstos son la parte fundamental del imperio de redes en Internet de Cisco. Debido al cambiante rostro de los negocios en el mundo de Internet, Cisco permanece a la vanguardia de las necesidades tecnológicas y de redes al abrazar las tecnologías actuales de negocios e invertir en lo que piensan que serán las tecnologías populares del futuro.

Una de esas áreas está en el campo de las comunicaciones de negocios. Hasta ahora, las comunicaciones se habían manejado a través de un sencillo teléfono que se encontraba en un rincón del escritorio, por correo electrónico o simplemente alzando la voz por encima de los canceles del cubículo. Voz sobre IP (VoIP, Voice over IP) es una forma de fusionar los servicios telefónicos en la red IP de la organización. Los beneficios de esto vienen no sólo desde el punto de vista monetario (cuando instrumentan soluciones VoIP, las empresas pueden ahorrar grandes sumas, sobre todo cuando se toma en cuenta lo que cuestan las llamadas locales y de larga distancia nacional e internacional), sino que también pueden hacer las comunicaciones más sencillas y fáciles.

En este capítulo, veremos más de cerca los productos y servicios de contacto IP de Cisco, incluidos VoIP y su sistema Cisco Unified Communications, que se supone que cambiará la forma en que las empresas se comunican (por lo menos es lo que Cisco espera).

VoIP

Si es posible entregar música, video y otros contenidos multimedia a través de interconexiones, ¿por qué no realizar conversaciones telefónicas por la misma vía? Quizá no sea sorprendente que Cisco posea toda una línea de productos que permiten la interacción VoIP.

Uno de los mayores beneficios para VoIP es algo que atraerá a todos los integrantes de la organización: ahorros en costos. Es preciso considerar los beneficios que recibió el Minnesota Department of Labor and Industry. El sistema telefónico del departamento fue armado con equipos provenientes de cinco sistemas de propietario. Luego de explorar las opciones de reemplazo, en el otoño de 2000 decidieron buscar una solución VoIP. El departamento instaló un sistema VoIP con 300 teléfonos, a un costo de 435 000 dólares.

Después de tres años, los beneficios eran numerosos. El departamento recortó su facturación telefónica en más del 50% (de 21 700 dólares a menos de 10 000 dólares). En el 2003, se agregaron siete nuevos lugares al despliegue VoIP del departamento y, hoy en día, muchas agencias más del gobierno de Minnesota ya se agregaron al sistema VoIP.

Además, Gartner, la firma de investigaciones, estima que los embarques de telefonía VoIP pasarán de 56% del mercado, con un valor de 2 000 millones de dólares, a más del 97% del mismo, con un valor de 4 700 millones de dólares, en el 2007.

Aunque se está volviendo muy popular, VoIP no siempre es una forma perfecta de librarse de los teléfonos de escritorio en la oficina, pero sí es una tecnología viable que evoluciona con gran rapidez. Existen grandes probabilidades de que usted, si es que no lo está haciendo ahora, estará empleando VoIP para comunicarse con una sucursal, o incluso con un antiguo amigo de la secundaria que vive del otro lado del continente. Vaya, con empresas como Vonage (www.vonage.com) que están vendiendo VoIP residencial con llamadas ilimitadas locales y de larga distancia por una cuota de menos de 25 dólares al mes, es muy posible que vaya a tener un equipo VoIP en su hogar en un futuro no muy distante.

En esta sección, analizaremos los pormenores y la tecnología que rodean a VoIP, y luego observaremos las soluciones y equipo de Cisco para proporcionar servicios de telefonía a través de las redes IP.

Introducción

Una de las primeras promesas de Internet fue la perspectiva de hacer llamadas gratuitas de larga distancia. En teoría, una computadora codificaría las llamadas, las transmitiría por Internet y la computadora receptora las decodificaría. Además, sólo habría necesidad de un tipo de red, la red del Internet Protocol (IP, protocolo Internet). Esto eliminaría la necesidad de dos redes exclusivas para voz y datos. No obstante, en la práctica esta tecnología aún debe recorrer un largo camino.

El principal problema es de recursos. A fin de que la llamada pueda llegar a su destino, los paquetes debían recibirse en el orden correcto, o de lo contrario las llamadas por Internet se recibirían como galimatías. Con demasiada frecuencia, los paquetes se recibían en orden aleatorio. El resultado era demora, pérdida de paquetes y orden disperso, lo que con el tiempo hizo que las llamadas fueran difíciles de entender y reveló que el sistema no era la panacea que todos habían esperado que fuera.

Cómo funciona

¿Qué ocurre cuando se hace una llamada VoIP? Se observará el proceso, como se ilustra en la figura 9-1, siguiendo los pasos por número:

1. Se levanta el receptor y el Private Branch Exchange (PBX, intercambio de ramal privado) genera un tono de marcar.

NOTA Un PBX es un instrumento que se ubica dentro de una organización que dirige las llamadas telefónicas que se reciben hacia la dirección deseada. También proporciona características adicionales, como correo de voz o redireccionamiento de llamadas. En este capítulo hablaremos más del PBX.

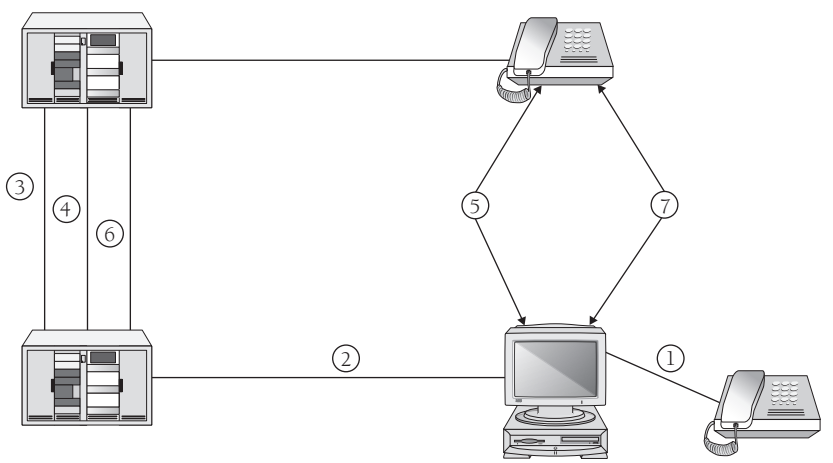


Figura 9-1. Los pasos numerados demuestran el funcionamiento de VoIP.

2. El usuario marca el número telefónico (el PBX almacena los números).
3. Una vez que se ingresa una cantidad suficiente de dígitos para coincidir con un patrón configurado de destino, el número telefónico se diagrama en el anfitrión IP. Este paso se lleva a cabo utilizando un mapa del plan de marcado. En este punto, el anfitrión IP realiza una conexión con el número telefónico de destino o con un PBX, que completará la llamada hasta su destino.
4. Se establece un canal de transmisión y recepción cuando la aplicación de la sesión ejecuta un protocolo como el Session Initiation Protocol (SIP, protocolo de inicio de sesión) o el protocolo de sesión H.323. (En páginas posteriores de este capítulo se hablará con mayor detalle de los protocolos SIP y H.323.) Si un PBX está manejando la llamada, la dirige hacia el teléfono de destino. Si se ha configurado el Resource Reservation Protocol (RSVP, protocolo de reservación de recursos), se hacen llamadas RSVP.

NOTA RSVP "aclara el camino" entre los enrutadores de los dos teléfonos. Cisco llama a esto "reservar recursos". RSVP es una forma de lograr la calidad deseada de servicio en una red IP.

5. Los códecs se habilitan en ambos extremos de la conexión, y la conversación se realiza utilizando el conjunto de protocolos RTP/UDP/IP.

NOTA Los códecs son equipo de hardware o programas de software que traducen señales analógicas de voz a paquetes IP que puede transmitirse por la red.

6. Cualquier indicador de llamada en progreso (u otro tipo de señal que es posible transportar en la banda) se conecta a través de la ruta de voz una vez que se establece el canal de audio de extremo a extremo.
7. Una vez que concluye la llamada telefónica (es decir, cuando uno de los dos interlocutores cuelga su aparato), se rompen las reservaciones RSVP (si es que se utilizaron), la conexión se rompe y las sesiones terminan. En este punto, cada extremo queda desocupado, en espera de una señal de "descolgado" o una llamada de teléfono IP entrante.

Además de transportar los paquetes, la red IP debe asegurar también que la conversación es transportada por los medios de comunicación, de tal manera que se escuche con la mejor calidad de voz. Si los paquetes se reciben en un orden diferente de aquel en que se enviaron, entonces la conversación será confusa y, a la larga, truncada e inútil. Por último, el flujo de paquetes de telefonía IP debe convertir a otro formato en una gateway. Esto es necesario para propósitos de interoperación con un sistema multimedia basado en IP, o si la llamada telefónica termina en un sistema convencional de telefonía pública.

Desarrollo de redes VoIP

Existen tres tipos básicos de VoIP. Se diseñan en torno a las necesidades específicas del usuario y para atender un mercado específico:

- ▼ **Desvío simple de tarifa** El uso más sencillo para el VoIP es emplearlo para hacer llamadas telefónicas sin tener que utilizar la red telefónica conectada al sistema público (PSTN). Esto es ideal si se desea emplear IP para transportar las llamadas entre distintas oficinas dentro de la red corporativa. El diseño requiere un cambio mínimo a las infraestructuras existentes de PBX, cableado y aparatos; su desarrollo es relativamente sencillo y no hay problemas de integración con la red telefónica conectada al sistema público.
- ■ **Telefonía total IP** Este diseño relega al cesto de la basura los sistemas existentes de voz. Encima de los escritorios ya no habrá aparatos telefónicos convencionales (en vez de ello, se cambiarán por teléfonos IP que se conectarán a puertos Ethernet). Se utilizarán los servidores LAN para proporcionar casi todas las características que el PBX brinda hoy en día. Ésta es la meta final de VoIP y no algo que comenzará a ocurrir en breve.
- ▲ **PBX con capacidades IP** Esta solución no es tan robusta como una telefonía total IP, pero se contará con una mezcla de funcionalidades. No es preciso cambiar los cables o aparatos existentes, sino que se actualizará el PBX de manera que los sistemas básicos de la organización podrán hablar los protocolos de telefonía IP. Los usuarios de PBX podrán comunicarse con otros usuarios de telefonía, pero la limitación es que el PBX deberá depender de las gateways de telefonía IP para comunicarse con el sistema telefónico público convencional.

La solución más sencilla de instrumentar es la desviación simple de tarifa, de modo que se verá más de cerca su funcionamiento, y luego se agregarán algunos de los elementos de los otros dos conceptos de diseño.

Desviación simple de tarifa

La instrumentación de las soluciones VoIP de desviación de tarifa es razonablemente sencilla. Antes de comenzar a realizar cambios, veamos más de cerca los elementos con los que es más probable que tenga que comenzar. En la figura 9-2 se ilustran tres PBX conectados.

Un PBX es un instrumento que se localiza dentro de una organización y que conecta las llamadas telefónicas que llegan por líneas troncales de la red telefónica conectada al sistema público a las extensiones designadas. Asimismo, los PBX pueden conmutar las llamadas a las extensiones que se ubican en otros PBX conectados. Casi todas las interconexiones de PBX son digitales, e incluso podrían ser circuitos T1, dedicados al propósito específico de interconectar PBX. No obstante, de manera típica, se trata de canales establecidos sobre una espina dorsal de Time Division Multiplexing (TDM, multiplexaje por división de tiempo). Éste divide el ancho de banda entre la voz y los datos.

El problema de tener líneas exclusivas para voz y TDM para servicios múltiples es que resulta preciso asignar de manera permanente un ancho de banda para cada circuito de voz, aunque no estén en uso. Una mejor manera de administrar los recursos consiste en dividir el tráfico en paquetes, de modo que todo el tráfico pueda reunirse y emplear el ancho de banda de manera más eficiente. Aquí es donde entra en escena VoIP.

La manera más sencilla de desplegar una solución VoIP consiste simplemente en desconectar las líneas al PBX y conectarlas a una unidad separada que convierta las señales de voz y las transporte en un formato IP. A estas unidades (como el adaptador telefónico analógico ATA 186 de Cisco) se les conoce como *relevadores VoIP* y se conectan a un enrutador que las transportará por una red IP, como se ilustra en la figura 9-3.

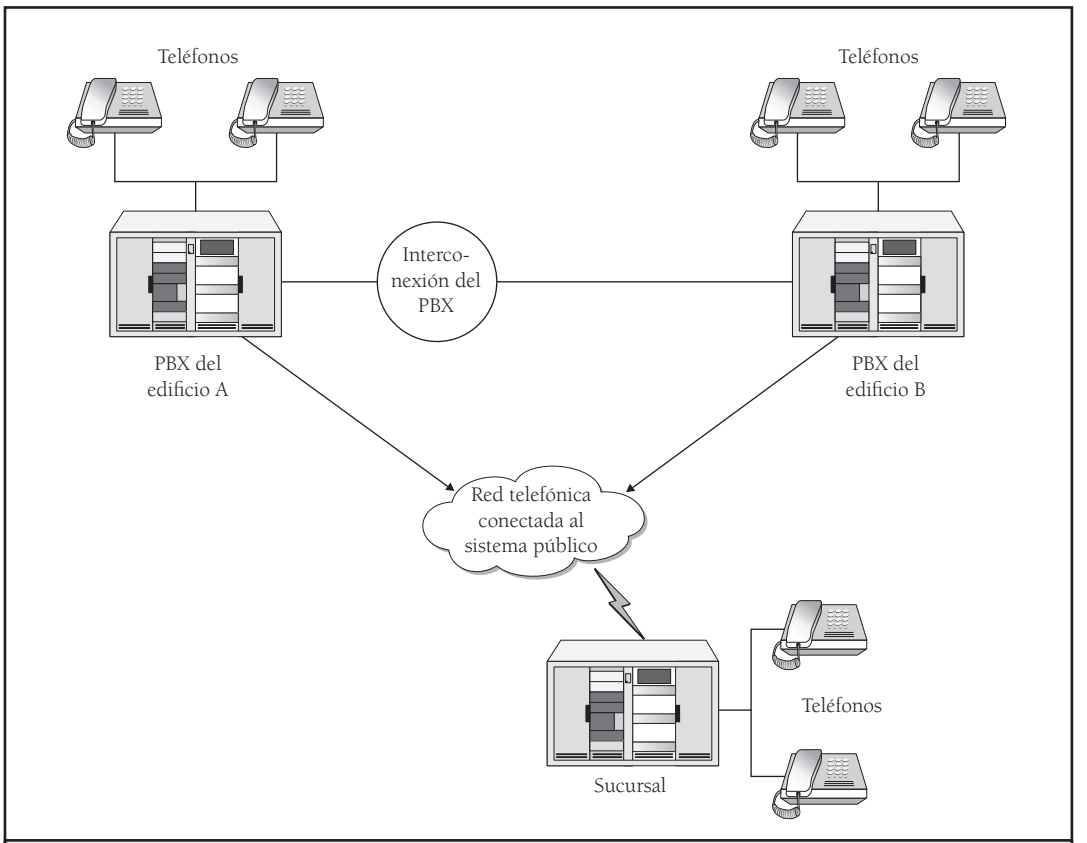


Figura 9-2. Esta red telefónica existente es común para muchas organizaciones.

Sin embargo, no es preciso comprar por separado un relevador VoIP y un enrutador. Varios enrutadores Cisco (por ejemplo, las series 1700, 2600 y 3600) proporcionan interfaces directas a PBX. Pero si se desea un relevador y enrutador VoIP por separado, es posible configurar la solución VoIP de esa manera.

Sin importar la ruta que elija, existen tres temas de diseño básico que es preciso abordar:

- ▼ Asegúrese de que la gateway VoIP recibirá y transmitirá información de señales suficiente para apoyar las características en uso en el PBX.
- ■ Asegúrese de conocer el tipo de normas que emplea su solución. Aunque algunos productos prometen compatibilidad con H.323, existe aún un número de esquemas de propietario.
- ▲ Asegúrese de determinar cómo se abastecerá la calidad necesaria de voz. Este tema se reduce a una combinación del esquema de codificación que emplea y las capacidades QoS de su red.

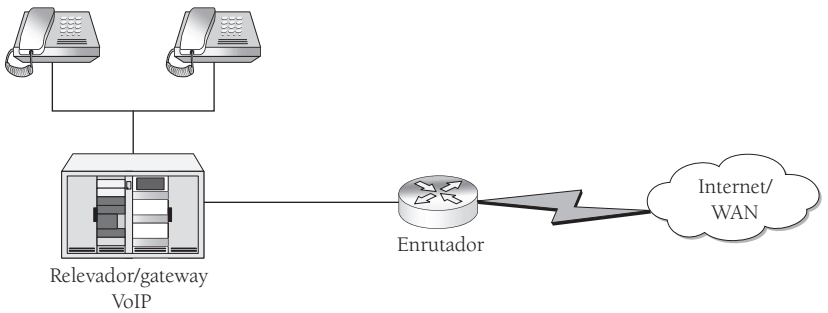


Figura 9-3. La conexión de teléfonos a un relevador VoIP y a un enrutador proporciona conectividad VoIP.

Solución VoIP

El sistema de desviación simple de tarifa que se analizó antes es un escenario sencillo y económico que es posible lograr con pocos o ningún problema. Pero si se desea ser un poco más aventurero, considere el diseño de la figura 9-4.

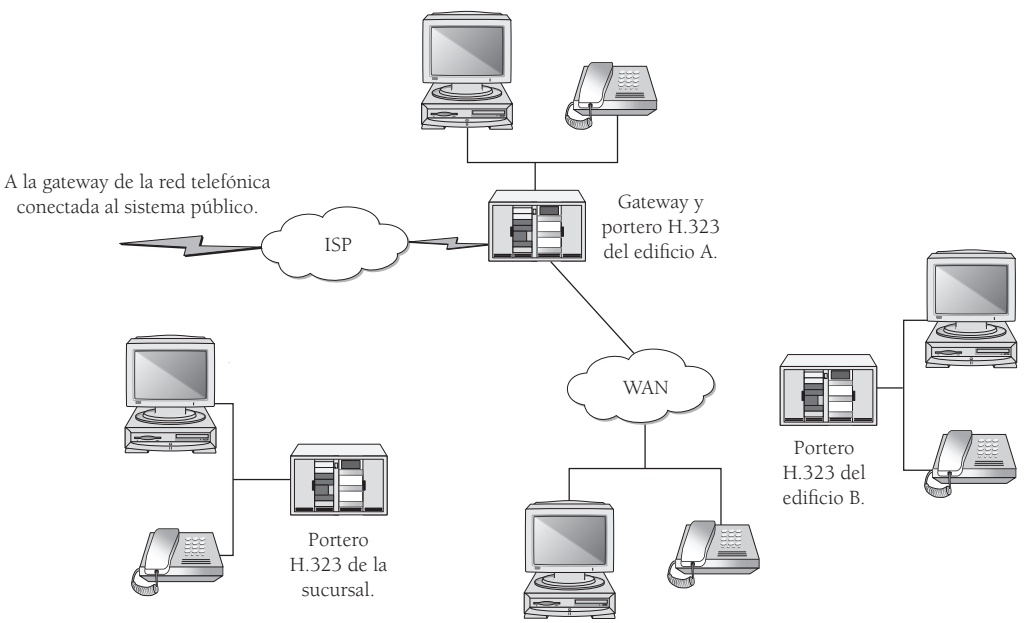


Figura 9-4. Con una solución de telefonía IP completa, las computadoras personales y los teléfonos se conectan a la LAN.

En una solución completa de telefonía IP, todos los equipos para el usuario final (computadoras personales y teléfonos) se conectan a la LAN. El teléfono que los usuarios conocerán y amarán puede ser de uno de dos tipos:

- ▼ Teléfonos físicos IP, que se ven y actúan igual que los teléfonos convencionales, excepto que están enchufados a la red.
- ▲ Teléfonos IP de software, que dependen del software del cliente que opera en la computadora personal.

Observe la figura 9-5. Por ejemplo, si Pedro, de servicio de mantenimiento, quiere llamar a Patricia de contabilidad, toma el teléfono IP y se comunica con ella a través de la LAN A utilizando una conexión IP. Sin embargo, si Pedro necesita ordenar un tambo de cera para

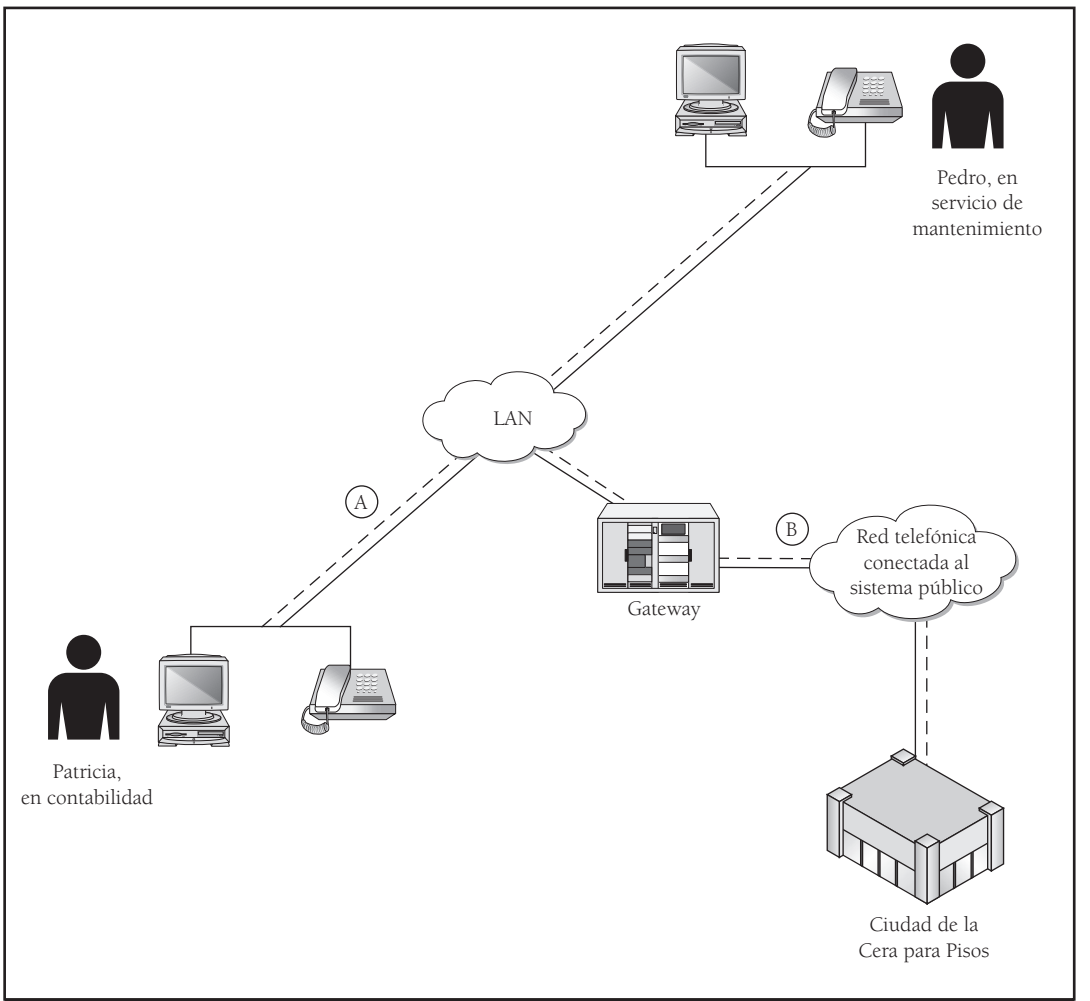


Figura 9-5. Las llamadas telefónicas IP se conectan dentro y fuera de la red IP con distintos equipos.

pisos, la llamada pasa por la red utilizando una conexión B de IP y luego se vincula a un gateway. La *gateway* (como el Cisco EGW 2200 Enterprise Gateway) es un aparato que vincula las llamadas VoIP a la red de telefonía pública.

Por último, existen servidores que soportan la telefonía IP. Estos servidores proporcionan las funciones básicas de establecimiento de llamadas y las características avanzadas que los usuarios consideran implícitas en los PBX tradicionales, como correo de voz, llamada en espera y redireccionamiento de llamadas. Veamos más de cerca los teléfonos, gateways y servidores de IP.

Teléfonos IP En su forma más sencilla, puede establecer un teléfono IP conectando una bocina y un micrófono a la computadora personal. Sin embargo, las personas esperan que sus teléfonos se vean y se sientan como teléfonos. Como se mencionó antes, existen teléfonos IP de hardware y de software. Esa "sensación de teléfono" puede lograrse con un aparato telefónico que hable IP y que pueda conectarse de manera directa a un conmutador. Como opción, los usuarios pueden enchufar de manera directa un auricular especialmente diseñado a la computadora personal para aprovechar la solución de software.

En páginas posteriores de este capítulo, hablaremos del sistema de Cisco Unified Communications. Muchos de los teléfonos IP para esa solución no sólo se ven como teléfonos "normales", sino que también tienen pantallas de video y displays al estilo de "Los Supersónicos".

Cada uno de estos teléfonos ofrece los mismos tipos de características que un teléfono conectado a un PBX. Naturalmente, estas soluciones tienen también algunas desventajas. Los teléfonos de hardware IP necesitarán una conexión en el conmutador (atención, es posible quedarse sin conexiones con gran rapidez), y también necesitan su propia fuente de poder. Algunos conmutadores, como el Cisco Catalyst 6500, la proporcionan.

Es posible evitar estos peligros utilizando un teléfono IP basado en software. Esto se logra conectando un aparato a un puerto serial o USB, o conectando un viejo teléfono analógico a una tarjeta de computadora personal o a un adaptador externo. En páginas posteriores de este capítulo se hablará con más detalle de algunos de los teléfonos VoIP de Cisco y de los teléfonos de software.

Si decide emplear el teléfono IP basado en software (o teléfono de software), deberá recibir software de cliente que soporte la telefonía IP. Este software puede ser independiente, basado en estándares (es preciso asegurarse de comprar uno que coincida con las especificaciones del teléfono), o como parte de un paquete, como NetMeeting de Microsoft.

Al seleccionar un teléfono IP, existen tres puntos que es preciso tener presentes:

- ▼ Al considerar teléfonos IP de hardware, asegúrese de que el aparato no limitará su capacidad de integración con el entorno de su máquina de escritorio. Por ejemplo, necesita asegurarse de que cuenta con suficiente ancho de banda y puertos de conexión de equipo para soportar a las computadoras y el VoIP.
- ■ Asegúrese de que los teléfonos soportan los estándares apropiados de códecs y señalización.
- ▲ Asegúrese de que el teléfono y la red podrán compartir prioridades de QoS.

Gateways Las gateways sirven como interfaces entre las llamadas telefónicas de la red telefónica conectada al sistema público y la telefonía IP. La red telefónica conectada al sistema público consta de dos redes separadas: una para transportar las conversaciones de voz y otra para hacer lo propio con la información de señales (utilizando el protocolo SS7).

Hagamos una breve pausa para considerar algunos de los puntos básicos del sistema de telefonía pública que será importante conocer, para comprender la funcionalidad de las gateways:

- ▼ **Oficina central** Donde los teléfonos locales se conectan por primera vez a la red pública.
- ■ **Conmutador de oficina central** El conmutador local en la oficina central.
- ▲ **Conmutador tándem** Conmutadores que interconectan entre los conmutadores de la oficina central en una red de área local.

Un conmutador de oficina central conecta las troncales de voz y SS7 a los Signal Transfer Protocols (STP, protocolos de transferencia de señal). Éstos son los conmutadores de mensajes que dirigen la información de señales SS7. Estas dos troncales se mantienen separadas porque eso facilita el establecimiento y eliminación de llamadas de voz. También aligera la carga de la red durante los periodos de uso pico. El SS7 también es necesario para los números 800 y 888, y tiene ventajas como redireccionamiento de llamadas, identificación de llamadas y devolución de la última llamada.

El uso de SS7 no es necesario para una conexión de telefonía IP a un gateway de la red telefónica conectada al sistema público, mientras haya señalización en banda en las troncales de voz, pero esto sirve sólo para una llamada telefónica desde un equipo de telefonía IP a un teléfono en la red telefónica conectada al sistema público. Si se desea una funcionalidad adicional (como redireccionamiento de llamadas y otras), es necesaria otra gateway: la IP SS7 a IP Telephony Gateway.

Cisco ofrece varios productos de gateway para su uso en las soluciones VoIP, incluidos los gateways universales de las series AS5300, AS5400 y AS5800. Además, varios enrutadores incluyen funcionalidad de gateway, desde la serie 800 hasta la 7500.

Servidores Una llamada telefónica básica IP ocurre cuando un teléfono IP se conecta con otro. Sin embargo, existen varias funciones "tras bambalinas" que es preciso administrar, incluidas características como enrutamiento de llamadas y facturación. Ninguno de los usuarios finales puede realizar ninguna de estas funciones; más bien, deben realizarse en un servidor de telefonía IP (o varios, dependiendo del tamaño de la red). Bajo el protocolo H.323, un portero realiza este conjunto de funciones. El H.323 y el portero se explicarán con mayor detalle en páginas posteriores de este capítulo, en la sección "H.323". También se hablará del protocolo más reciente, el Session Initiation Protocol (SIP, protocolo de inicio de sesión). Los porteros también incluyen soporte para temas adicionales como mensajes y conferencias de voz en el mismo servidor de telefonía IP.

Codificación

Cuando habla en un teléfono, hace que las moléculas de aire se muevan; éstas rebotan en un micrófono y se convierten en una señal eléctrica, que a su vez es enviada por la red, donde vibra en el altavoz del otro teléfono. Estas vibraciones mueven las moléculas de aire que completan la transformación del sonido en electricidad y luego de nuevo a sonido.

En el caso de VoIP, es preciso agregar una capa adicional al proceso. No es suficiente transportar la señal eléctrica; debe transformarse de un formato analógico a uno digital. Esta conversión es exactamente lo que hace la diferencia entre los discos LP de acetato (¿los recuerda?) y los compactos.

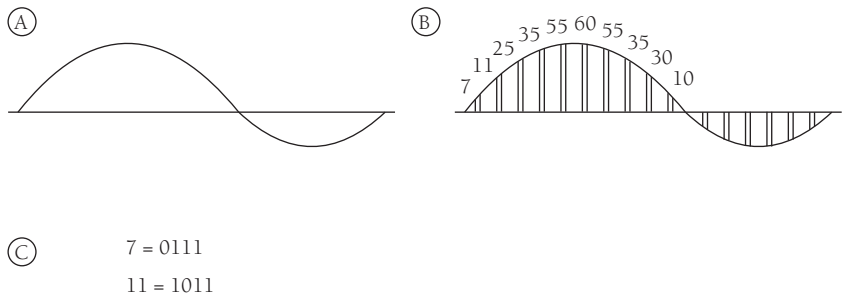


Figura 9-6. Una onda analógica se convierte a un flujo de datos digital al medir "rebanadas" regulares.

En la figura 9-6 se ilustra una onda analógica, en que (A) representa cómo se ve el sonido cuando se mueve por primera vez en un micrófono. A continuación (B) (la onda) se muestrea en intervalos regulares, la señal se muestrea a su vez y los números (C) se convierten en una serie de ceros y unos. A este proceso se le conoce como *codificación de voz,* y el software o al aparato que se emplea para codificar (y después decodificar) la señal se le conoce como *códec.* Por supuesto, cuanto más pequeño sea el intervalo entre muestras, mejor será la calidad del sonido. Sin embargo, cuanto más frecuente sea el muestreo, consumirá más ancho de banda.

Una buena regla práctica cuando se muestrea, es hacerlo a una tasa de por lo menos 2.2 veces la frecuencia máxima que se representa en la señal básica. La voz humana emplea frecuencias que van de los 300 Hz a los 4 KHz. Para simplificar las operaciones matemáticas, se puede utilizar una tasa de muestreo de 8 000 veces por segundo. Por ejemplo, si se utilizan 8 bits para representar la fuerza de la señal, entonces se necesitará un ancho de banda de 8 bits, 8 000 veces por segundo, es decir, 64 Kbps. A esto se le conoce como Pulse Code Modulation (PCM, modulación del código de impulso) y es la forma más popular de codificar la voz en las redes de telefonía pública.

Los codecs proporcionan diversas calidades de habla. Esta calidad no es una cantidad finita; es más bien subjetiva. Lo que una persona pensaría que es un habla perfectamente clara podría sonar demasiado confuso y electrónico para otra. La forma de hacer que el subjetivo mundo de la calidad en el sonido sea más objetivo es por medio de la Mean Opinion Score (MOS, puntuación de opinión media). Al igual que las pruebas en grupos de un nuevo tipo de salsa de tomate, se reúne a oyentes para que juzguen la calidad de una muestra de voz y que luego la califiquen en una escala de 1 a 5, donde 1 es "malo" y 5 es "excelente". Luego se promedian estas puntuaciones para proporcionar la MOS de esa muestra.

En la tabla 9-1 se comparan diferentes códecs, sus tasas de bits, demora de compresión y calificaciones de MOS.

En la tabla 9-1, se usa la tasa de bits para describir la cantidad de datos que se envían por segundo. Recuerde que cuanto mayor sea ese valor, mejor será la calidad general. Observará que el código con la mayor tasa de bits (G.711) obtuvo la puntuación MOS más alta.

En segundo lugar se encuentra la demora de compresión. Ésta es la cantidad de tiempo que se requiere, en milisegundos, para codificar la señal. Se trata de un factor muy impor-

Método de compresión	Tasa de bits (Kbps)	Demora de compresión (ms)	Puntuación MOS
G.711 Pulse Code Modulation (PCM, modulación de código de impulso).	64	0.75	4.1
G.726 Adaptive Differential Pulse Code Modulation (ADPCM, modulación de código de pulso adaptativo diferencial).	32	1	3.85
G.728 Low-Delay Code Excited Linear Prediction (LD-CELP, código de predicción lineal de bajo retraso).	16	3 a 5	3.61
G.729 Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP, predicción lineal de código algebraico excitado de estructura conjugada).	8	10	3.92
G.729 x 2 Codificadores.	8	10	3.27
G.729 x 3 Codificadores.	8	10	2.68
G.729a CS-ACELP.	8	10	3.7
G.723.1 Multipulse, Multilevel Quantization (MP-MLQ, cuantización multipulso, multinivel).	6.3	30	3.9
G.723.1 Algebraic Code Excited Linear Prediction (ACELP, predicción lineal de código algebraico excitado).	5.3	30	3.65

Tabla 9-1. Comparación entre códecs VoIP.

tante por tomar en cuenta al seleccionar un códec, porque los tiempos de codificación demasiado prolongados harán que las conversaciones sean difíciles de entender.

No existe un "mejor" códec. Dependiendo de sus necesidades, habrá que equilibrar estas variables para obtener la mejor solución. Aunque G.711 tiene la puntuación MOS más elevada, también consume el mayor ancho de banda. G.723 consume diez veces menos ancho de banda que G.711, y está en un cercano tercer lugar en términos de puntuación MOS. Sin embargo, se requiere 40 veces menos tiempo para codificar la señal con G.723 que con G.711. Todos estos factores deben tomarse en cuenta cuando se seleccione un códec para la solución VoIP.

Calidad del servicio

La codificación no es la única forma de asegurar la calidad de voz. Debido a la forma en que funcionan las redes IP, es importante que los paquetes que contienen información VoIP lleguen y se decodifiquen en el mismo orden en que se enviaron, y sin retrasos mayores a 150 milésimas de segundo (ms). De lo contrario, la decodificación sería un galimatías carente de sentido.

En esencia, QoS (calidad del servicio) es un medio de asegurar que los paquetes que tienen prioridad (como los que contienen información VoIP) recorran la red más rápido que los de otras aplicaciones menos críticas.

Por lo general, la asignación de prioridades a los paquetes es menos importante para el trabajo en red de datos, que tolera más el desempeño variable en la red. Así, las redes no fueron diseñadas para asegurar que los paquetes se reciban con rapidez o en orden (algo de lo que a casi ninguna aplicación de datos le preocupa demasiado). Sin embargo, sin los mecanismos QoS instalados, la entrega aleatoria y lenta es la muerte de VoIP.

Es útil analizar la forma en que es posible instrumentar QoS teniendo presente a VoIP. Desde el punto de vista de diseño, existen también dos consideraciones a tomar en cuenta cuando se establece la forma de proporcionar el nivel deseado de QoS. En primer lugar, es preciso que determine las capacidades de la infraestructura de enrutadores y las actualizaciones que tendría que realizar para soportar la QoS que desea. A continuación, es preciso que se cerciore de que los sistemas finales de telefonía IP funcionarán con los mecanismos de QoS.

H.323

En el mundo de VoIP, existen varios protocolos importantes. H.323 es una recomendación general de la International Telecommunications Union (ITU), que establece los estándares para las comunicaciones multimedia sobre LAN que no cuentan con un mecanismo QoS. Por desgracia, estos tipos de redes son la norma en casi todas las organizaciones, que incluyen paquetes conmutados TCP/IP e IPX en las redes Ethernet, Fast Ethernet y Token Rings. Como tales, la norma H.323 es una tecnología importante para las aplicaciones basadas en LAN para comunicaciones multimedia. La norma cubre varias tecnologías, incluidos equipos independientes y tecnología de computadoras personales incrustadas, así como conferencias punto a punto y multipuntos. Además del hardware, H.323 aborda funciones de administración y control como control de llamadas, administración multimedia y administración de ancho de banda.

Importancia de H.323

La norma H.323 lo incluye todo, aunque permanece flexible y puede aplicarse a aparatos de mano básicos de voz o a estaciones de trabajo completas para conferencias en video. Existen varias razones por las que H.323 es un protocolo popular para VoIP:

- H.323 establece los estándares multimedia para las redes más importantes basadas en IP. Está diseñado para compensar las altamente variables latencias de LAN que existen en las redes basadas en IP. Al utilizar H.323, es posible utilizar las aplicaciones multimedia sin tener que reformar toda la red.

- Las LAN de IP son cada vez más poderosas. A partir de velocidades de 10 Mbps, luego 100 Mbps y hoy en día de 1 Gbps, cada vez son más las redes capaces de proporcionar el ancho de banda que requerirán las aplicaciones H.323.
- Las computadoras personales siguen haciéndose más potentes, debido a las mejoras constantes en los procesadores, la memoria y los chips de aceleración de multimedia.
- Si es necesario comunicarse entre dos tipos diferentes de redes, la norma H.323 permite la funcionalidad de redes de Internet.
- La cada vez mayor manejabilidad del trabajo en red puede limitar la cantidad de ancho de banda que consume la actividad multimedia. Con H.323, los administradores de red pueden limitar la cantidad de ancho de banda de red que está disponible para las conferencias. Para ser más eficientes en los recursos de red, el soporte de transmisión múltiple de H.323 reduce el consumo de ancho de banda.
- ▲ En un campo en el que abundan las tecnologías propietarias, H.323 posee el beneficio de que muchas empresas de cómputo y comunicaciones lo soporten. Intel, Microsoft, Cisco e IBM son algunos de los nombres más importantes que respaldan el H.323.

Beneficios clave de H.323

Existen varias razones por las que H.323 sobresale como la manera más popular de realizar conversaciones VoIP:

- ▼ **Estándares de códec** H.323 define los estándares para la compresión y descompresión de los flujos de datos de audio y video. Esto garantiza que los datos serán legibles si se transmiten entre los productos de diferentes fabricantes.
- **Independencia de red** H.323 está diseñado para operar en casi todas las arquitecturas más comunes de red. En la medida que evoluciona la tecnología de red y mejoran las técnicas de administración de ancho de banda, las soluciones basadas en H.323 podrán aprovechar estas capacidades mejoradas.
- **Independencia de plataforma y aplicaciones** Al igual que todos los estándares, H.323 no es dominio exclusivo de ningún proveedor de hardware o de sistema operativo. Además, H.323 no se limita a las computadoras personales. Las plataformas compatibles con H.323 vienen en varias formas, incluidos videoteléfonos, teléfonos con capacidad IP y televisión por cable.
- **Soporte multipunto** H.323 ya soporta multiconferencias, que pueden soportar conferencias con tres o más extremos sin requerir equipos especiales. Sin embargo, la inclusión de Multipoint Control Units (MCU, unidades de control multipunto) proporcionará un entorno más poderoso para albergar conferencias multipunto.
- **Administración de ancho de banda** Debido a que el tráfico generado por las aplicaciones de audio y video consume grandes cantidades de ancho de banda, existe la posibilidad de saturar aun las redes más robustas. H.323 aborda el problema con herramientas de administración de ancho de banda. Utilizando equipos de administración, los gerentes de red pueden establecer límites en la cantidad de conexiones concurrentes H.323 dentro de su red, o pueden limitar la cantidad de ancho de banda disponible para las aplicaciones H.323. Con una administración adecuada de recursos, ninguna red se necesitará hacer más lenta.

- **Soporte de transmisiones múltiples** Para las situaciones en que varias personas recibirán la misma transmisión, H.323 soporta el transporte de transmisiones múltiples. Por ejemplo, en el caso de un director general que transmite un discurso a varias oficinas filiales, la transmisión múltiple H.323 envía un solo paquete a todas las filiales. Aunque los datos siguen en la red de la oficina central de la empresa, no se duplican los datos, lo que ahorra recursos. Compare esto con la *transmisión unitaria,* que envía varias transmisiones punto a punto, y con la *transmisión,* que lo envía a todos los destinos. Emplear estos dos últimos tipos supone un uso ineficiente de la red, porque los paquetes se duplican de manera innecesaria. La transmisión múltiple emplea el ancho de banda de manera más eficiente porque todas las estaciones en la red leen el mismo flujo de datos.
- **Flexibilidad** No todas las computadoras de los usuarios son creadas de igual manera. Sin embargo, al emplear un equipo compatible con H.323, es posible conducir conferencias a través de una red que incluya varios extremos, cada uno de ellos con distintas capacidades. Por ejemplo, es posible escuchar una teleconferencia por un usuario cuya máquina está habilitada sólo para VoIP.
- **Conferencias en interconexiones** En el último ejemplo, hablamos de H.323 como un medio de comunicación a través de redes con diferentes equipos, pero H.323 no se limita a las computadoras personales de escritorio. Podrá emplearse en distintos tipos de arquitecturas de red, y emplea tecnología común de códec de diferentes estándares de videoconferencia para reducir al mínimo las demoras de transcodificación y, con ello, dar mejores resultados.

H.323 define cuatro componentes principales para un sistema de comunicaciones basada en red: terminales, gateways, porteros y unidades de control multipunto.

Terminales

Las terminales son los aparatos en el extremo final que emplean los clientes. La especificación requiere que todas las terminales soporten comunicaciones de voz, pero las de video y datos son opcionales. H.323 especifica la forma en que diferentes terminales de audio, video y datos trabajarán juntos.

Además, todas las terminales H.323 deben soportar H.245, que es un mecanismo que se emplea para negociar el uso y las capacidades de uso de canal. Asimismo, las terminales deben soportar otros tres componentes:

- El protocolo Q.931 para la señalización y establecimiento de llamadas.
- Registration/Admission/Status (RAS, registro/admisión/estado), un protocolo que se emplea para comunicarse con un portero.
- Soporte para RTP/RTCP para la secuencia de paquetes de audio y video.

Los componentes opcionales en una terminal H.323 son códecs de video, protocolos de conferencia de datos y capacidades MCU.

Gateways

La función principal de una gateway es servir como traductor entre los extremos de conferencia de H.323 y las redes telefónicas conectadas al sistema público. Esta función incluye la traducción entre los formatos de transmisión y entre procedimientos de comunicaciones.

Además, la gateway también traduce entre diferentes códecs de audio y video y realiza el establecimiento y terminación de llamadas en el lado de la LAN y en el de la red de circuito conmutado.

Pero las gateways son un componente opcional en una conferencia H.323. Una gateway no es necesaria si uno no se conecta a otras redes, ya que los extremos pueden comunicarse de manera directa con otros extremos en la misma LAN.

Aunque el estándar H.323 es muy completo, se dejan abiertas varias funciones de gateway para que sean determinadas por el fabricante. Por ejemplo, el estándar no establece cuántas terminales pueden conectarse a través de la gateway.

Portero

Aunque las gateways son parte opcional del conjunto H.323, los porteros son un componente crucial. Un portero es el punto central para todas las llamadas dentro de su zona y proporciona servicios de control de llamadas a los extremos registrados.

Los porteros realizan las siguientes funciones:

- ▼ Reducción de los alias LAN para las terminales y gateways a direcciones IP o IPX.
- ■ Administración de ancho de banda. Por ejemplo, si el administrador de red ha establecido un límite en el número de conexiones concurrentes H.323 o un umbral en el uso de ancho de banda, es el portero quien puede negarse a recibir más conexiones una vez que se traspasa el umbral.
- ▲ Control de acceso a la LAN para las terminales y gateways H.323.

Los porteros sirven a la función opcional de enrutar las llamadas H.323. Enrutar las llamadas a través de un portero permite manejarlas con mayor eficacia y eficiencia. Esta característica tiene especial importancia en el nivel de proveedor de servicios, porque necesitan la capacidad de facturar las llamadas que se colocan a través de la red. Asimismo, esto puede ayudar a equilibrar los recursos de red, porque un portero capaz de enrutar llamadas H.323 puede tomar decisiones acerca de la administración de múltiples gateways.

No es indispensable un portero para un sistema H.323 funcional. Sin embargo, si un portero está presente en la red, las terminales deben emplear sus servicios de traducción de la dirección, control de las admisiones y de ancho de banda, y administración de zona.

Unidades de control multipunto

Para las conferencias entre tres o más usuarios, se emplea la unidad de control multipunto (MCU). Una MCU consiste de un controlador multipunto (MC), que es necesario, al igual que los procesadores multipunto (MP). Es posible albergar las capacidades MC y MP en un componente exclusivo o bien ser parte de otros componentes H.323.

El MC maneja las negociaciones H.425 entre todas las terminales y establece las capacidades comunes de audio y video. El MC se utiliza para manejar los recursos de conferencia determinando cuánto flujo de audio y video debe ser transmisión múltiple.

Sin embargo, el MC no controla en forma directa cualquiera de los flujos de los medios. Esta tarea es el dominio del MP, que mezcla, conmuta y procesa audio, video y datos.

SIP

Una opción a H.323 que está poniéndose de moda en la comunidad VoIP es el Session Initiation Protocol (SIP, protocolo de inicio de sesión). SIP es el estándar IETF (Internet Engineering Task Force) para las conferencias en multimedia a través de IP. SIP es un protocolo de control de capas de aplicación, basado en ASCII, que establece, mantiene y concluye las llamadas entre dos o más terminales.

En la tabla 9-2 se resaltan algunas de las funcionalidades del SIP.

Función	Descripción
Resolver la ubicación de los extremos de destino.	SIP soporta resolución de dirección, mapeo de nombres y redireccionamiento de llamadas.
Establecer las capacidades de medios de comunicación del extremo de destino.	Esto se logra utilizando el Session Description Protocol (SDP, protocolo de descripción de sesión). SIP determina el "nivel más bajo" de servicios comunes entre los extremos y las comunicaciones sólo se realizan utilizando las capacidades de medios de comunicación soportadas en ambos extremos.
Determinar la disponibilidad del extremo de destino.	Si no es posible completar una llamada porque el objetivo no está disponible, SIP determina si el objetivo ya está en el teléfono o si no respondió en el número asignado de llamadas. Por último, regresa un mensaje explicando por qué la llamada no tuvo éxito.
Establecer una sesión entre el extremo de origen y el de destino.	Si es posible completar la llamada, SIP establece una sesión entre los extremos. SIP también soporta cambios a mitad de llamada, como la adición de otro extremo a la conferencia o el cambio de una característica de medio de comunicación o códec.

Tabla 9-2. Funcionalidad del SIP (*continúa*).

Función	Descripción
Manejar la transferencia y terminación de llamadas.	SIP soporta la transferencia de llamadas de un extremo a otro. Durante una transferencia de llamadas, SIP simplemente establece una sesión a un nuevo extremo y finaliza la sesión entre la parte transferida y la que transfiere.

Tabla 9-2. Funcionalidad del SIP (*conclusión*).

SIP es un protocolo de igual a igual, lo que quiere decir que no es necesario un servidor dedicado para administrar las sesiones. En una sesión los iguales se conocen como *User Agents* (*UA, agentes de usuario*). Un UA tiene una de dos funciones en una conversación:

- ▼ **User Agent Client (UAC, cliente agente de usuario)** Aplicaciones de cliente que inician la solicitud de conversación del SIP.
- ▲ **User Agent Server (UAS, servidor agente de usuario)** Aplicaciones de servidor que ponen en contacto al usuario cuando recibe una solicitud SIP y luego devuelven una respuesta en nombre del usuario.

Un extremo SIP puede funcionar como UAC y como UAS. Sin embargo, en cualquier conversación, sólo funcionan como uno u otro. Un extremo funcionará como UAC o UAS, dependiendo de la UA que inició la solicitud.

Los componentes físicos de la red SIP pueden ser divididos en dos categorías: clientes y servidores. Los clientes SIP incluyen:

- ▼ **Teléfonos** Estos dispositivos pueden actuar como UAC o como UAS. Los teléfonos de software y Cisco SIP IP pueden iniciar las solicitudes de SIP y responder a éstas.
- ▲ **Gateways** Estos dispositivos controlan las funciones de llamada, que proporcionan varios servicios, incluida la traducción de funciones entre extremos de conferencia SIP y otros tipos de terminales. Esto incluye la traducción entre formatos de transmisión y entre procedimientos de comunicaciones. Además, la gateway realiza establecimiento y eliminación de llamadas.

Los servidores SIP incluyen:

- ▼ **Servidor Proxy** Este servidor proporciona funcionalidades como autentificación, autorización, control de acceso a la red, enrutamiento, retransmisión confiable de solicitudes y seguridad. Los servidores proxy reciben mensajes SIP y los envían al siguiente servidor SIP en la red.
- ■ **Servidor de redireccionamiento** Este servidor indica al cliente acerca del siguiente paso que debe dar un mensaje. Después, el cliente se pone en contacto con el servidor del siguiente paso o con el UAS de manera directa.

- **Servidor de registro** Este servidor procesa las solicitudes de los UAC para registrar su ubicación actual. Con frecuencia, los servidores de registro se colocan con un servidor proxy o de redireccionamiento.

SCCP

SIP es, en cierta forma, un monstruo destructor (en la misma medida que un protocolo VoIP podría ser considerado del mismo modo). A principios de 2006, Cisco retrocedió un paso de su Skinny Client Control Protocol (SCCP, protocolo delgado para el control del cliente), propiedad de ella, y permitió que el popular protocolo SIP fuera utilizado como parte de su sistema Cisco Unified Communications, de gran alcance.

SCCP es un protocolo propietario de control de terminales desarrollado por Selsius Corporation y comprado por Cisco a fines de la década de 1990. Actúa como conjunto de mensajes entre un cliente delgado y CallManager de Cisco.

Cisco ha respaldado SCCP (y sigue haciéndolo), pero ha seguido la funcionalidad SIP en las recientes soluciones VoIP. Esto es benéfico, porque permite que equipo y tecnología de otras marcas formen parte de la solución VoIP de Cisco.

Implementación

Existen varias formas en que es posible implantar VoIP en su organización. Ya sea que se trate de una persona que trabaja a distancia y que se conecta desde su hogar, o una oficina filial con un pequeño complemento de trabajadores que se conecta a la oficina central, existen varias formas de configurar una red para permitir capacidades VoIP.

Observemos de cerca los dos escenarios y hablemos de la forma de diseñar y construir redes habilitadas para VoIP.

Trabajo a distancia

Internet proporciona oportunidades excepcionales para descentralizar su oficina. En vez de hacinar a todo el personal en una colmena interminable de cubículos, la tecnología ha permitido a los trabajadores limitar su traslado a una caminata por la alfombra de la estancia. Al utilizar la tecnología VoIP, los trabajadores a distancia pueden comunicarse con la oficina central (o en todo caso, con cualquier lugar) sin impactar en la factura telefónica. VoIP resuelve gran cantidad de problemas para los trabajadores a distancia y para el personal de tecnología de la información de la organización, el problema más importante que resuelve es la necesidad de circuitos independientes para voz y datos.

Como se ilustra en la figura 9-7, al proporcionar un solo circuito de datos y equipo VoIP, es posible integrar la voz y los circuitos en un solo circuito. Asimismo, pueden estar tan bien integrados, que el trabajador a distancia puede llamar al operador de la empresa (simplemente marcando 0), al sistema de correo de voz y a otros recursos telefónicos. Es posible reducir el pago de teléfono al permitir que el trabajador a distancia haga llamadas VoIP a las oficinas remotas.

Pero VoIP no carece de problemas. El muro más alto que VoIP supone para el trabajador a distancia y (pequeña oficina/oficina en el hogar) incluye el ancho de banda y la administración de la red. Los usuarios necesitan ancho de banda suficiente para acomodar el tráfico

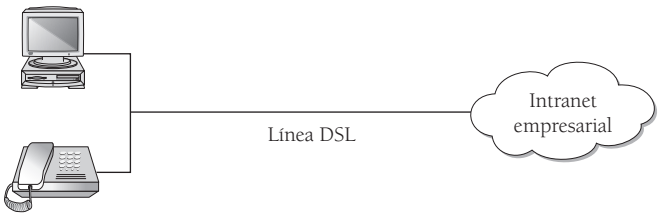


Figura 9-7. La combinación de voz y datos en un solo circuito ahorra dinero y recursos.

VoIP al tiempo que asignan prioridades, fragmentan y colocan en cola otros datos para proteger la integridad de la transmisión de voz. Si, como se ilustra en la figura 9-8, una llamada VoIP se atasca a la mitad de una gran transferencia de datos, la llamada podría sonar como si estuviera hablando con un extraterrestre de los que George Lucas inventó para la película *La guerra de las galaxias.*

Otro tema a considerar es que los circuitos hacia los trabajadores a distancia y en pequeñas oficinas/oficinas en casa deben mantener una conectividad de tiempo completo durante los horarios de negocios; de lo contrario, tal vez no puedan establecerse las llamadas al equipo del usuario. Por ejemplo, algunos equipos VoIP tratan de medir la latencia a un sistema remoto antes de establecer la llamada. Algunos sistemas son tan sensibles que los tiempos de establecimiento de llamada de ISDN pueden ser demasiado largos, con la consecuencia de llamadas rechazadas.

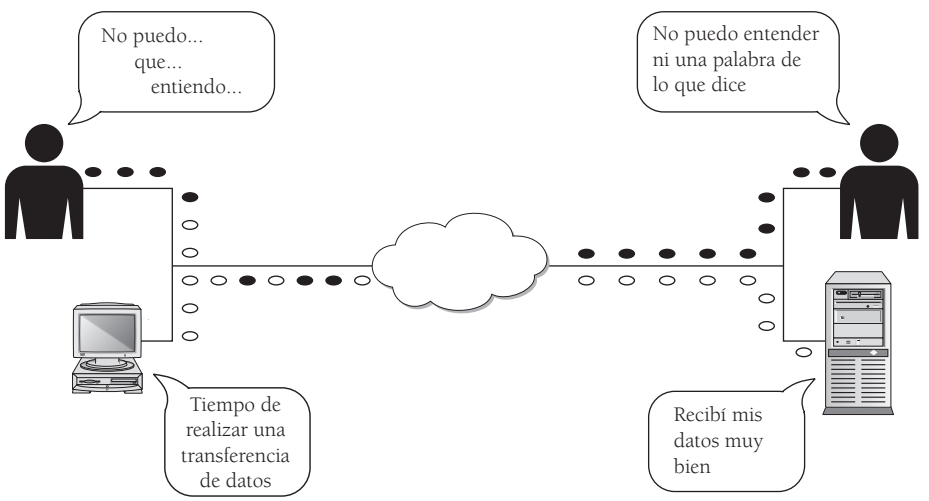


Figura 9-8. Enviar datos y VoIP al mismo tiempo puede interrumpir una llamada telefónica.

La mejor solución para estos asuntos (asignación de prioridades a paquetes y conectividad de tiempo completo) requiere el uso de, por lo menos, ISDN o DSL (Digital Suscriber Line, línea de suscriptor digital). No obstante, ISDN de tasa básica es un vínculo de sólo 128 Kbps, en tanto que DSL puede superar 1 Mbps.

Sucursales

El mejor lugar para instrumentar una solución VoIP es en las sucursales. Son ideales porque suelen tener un número pequeño de usuarios y no generan grandes volúmenes de tráfico. Además, estas oficinas son los sitios con mayores probabilidades de obtener beneficios de las ventajas de la gratuidad de VoIP como reemplazo para los servicios de larga distancia. Por lo general, las sucursales emplean líneas de alta velocidad como DSL o T1 para su conectividad. En la figura 9-9 se muestra un ejemplo de configuración.

Al igual que con todo lo demás, existen algunos ejemplos en los que todo encajará en su sitio de manera perfecta. Por ejemplo, es posible que las sucursales de su organización alberguen a varios centenares de empleados, y la implantación de VoIP puede crear algunos retos de infraestructura. Además, si la oficina remota ya está equipada con un PBX, no hay mucha necesidad de agregar equipo nuevo. Asimismo, si la organización enruta las llamadas de larga distancia a través de un circuito dedicado de costo fijo, no habría grandes ahorros para las oficinas generales.

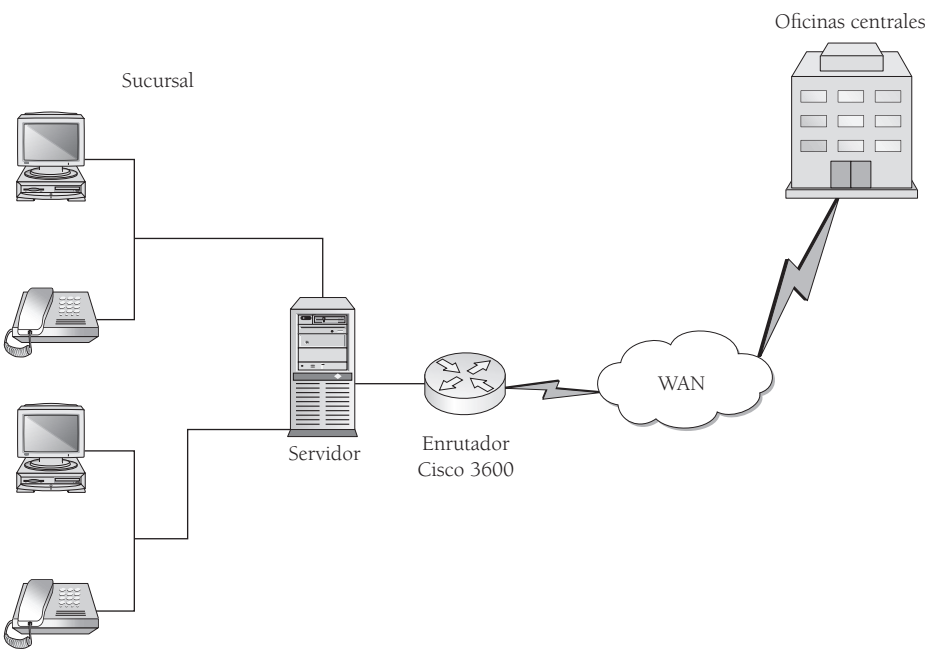


Figura 9-9. Las sucursales son excelentes lugares para implantar soluciones VoIP.

En los casos en que de verdad VoIP se gana su reputación como opción de larga distancia es al conectar oficinas a través de Internet. Su organización reconocerá considerables ahorros en costos al adquirir servicios garantizados de un ISP y luego enrutando las llamadas VoIP a través de esa conexión, en vez de pagar cuotas de larga distancia o comprando una red dedicada propia.

Al implantar VoIP en una sucursal, también es posible utilizar el plan de marcado, el correo de voz y otras características corporativas por una cantidad menor de dinero que el costo de un PBX adicional.

CISCO UNIFIED COMMUNICATIONS (COMUNICACIONES UNIFICADAS DE CISCO)

Las redes IP en general, e Internet en particular, han hecho de las comunicaciones una mezcla de disponibilidad. Ponerse en contacto con alguien es tan sencillo como enviar un correo electrónico, un mensaje instantáneo, una llamada IP o incluso una conferencia en video. Utilizar una red IP para ponerse en contacto con alguien es como abrir una bolsa de caramelos (hay demasiadas opciones). Sin embargo, al igual que la bolsa de caramelos, demasiadas opciones pueden ser un exceso. Mientras muchas barras de caramelo pueden hacer que uno se enferme, un exceso de métodos de comunicación puede representar un dolor de cabeza.

Se requieren diferentes aplicaciones para hacer una llamada de telefonía IP, enviar un correo electrónico o transmitir un mensaje instantáneo. Hasta ahora, no había un método para combinar todos estos modos de comunicación. Al ver la necesidad de hacer que converjan todas estas aplicaciones, Cisco introdujo su solución, Cisco Unified Communications.

Cisco Unified Communications es un conjunto de productos de voz, video y datos para ayudar a las organizaciones de todos los tamaños a comunicarse con mayor eficacia.

En la figura 9-10 se muestra la forma en que los componentes de presencia, localización e inteligencia de proceso de llamadas de Cisco Unified Communications trabajan en conjunto para proporcionar la siguiente generación de comunicaciones de negocios.

Cisco Unified Communications es una plataforma abierta y extensible para las comunicaciones en tiempo real. Utiliza la red de computadoras como plataforma de servicio para ayudar a los usuarios a llegar al recurso correcto desde la primera vez, al proporcionar información de presencia y preferencia a los usuarios de la organización.

"Esto lo cambia todo"

Si pasa cinco segundos con Cisco Unified Communications, escuchará los esfuerzos del departamento de mercadotecnia, con su eslogan "Esto lo cambia todo". La frase pasa de moda con bastante rapidez, pero es preciso darle el crédito a Cisco (de hecho, el sistema sí lo cambia todo).

Los impulsos detrás de Comunicaciones Unificadas de Cisco es un esfuerzo, por parte de Cisco, para cambiar el rostro de las comunicaciones de negocios, no sólo para satisfacer una necesidad existente.

Las comunicaciones son críticas para las organizaciones y han sido desarrolladas y desplegadas a partir de las necesidades. Es decir, las personas necesitan hablar con otras personas, de modo que en todos los escritorios se encuentra un teléfono. Las personas necesitan

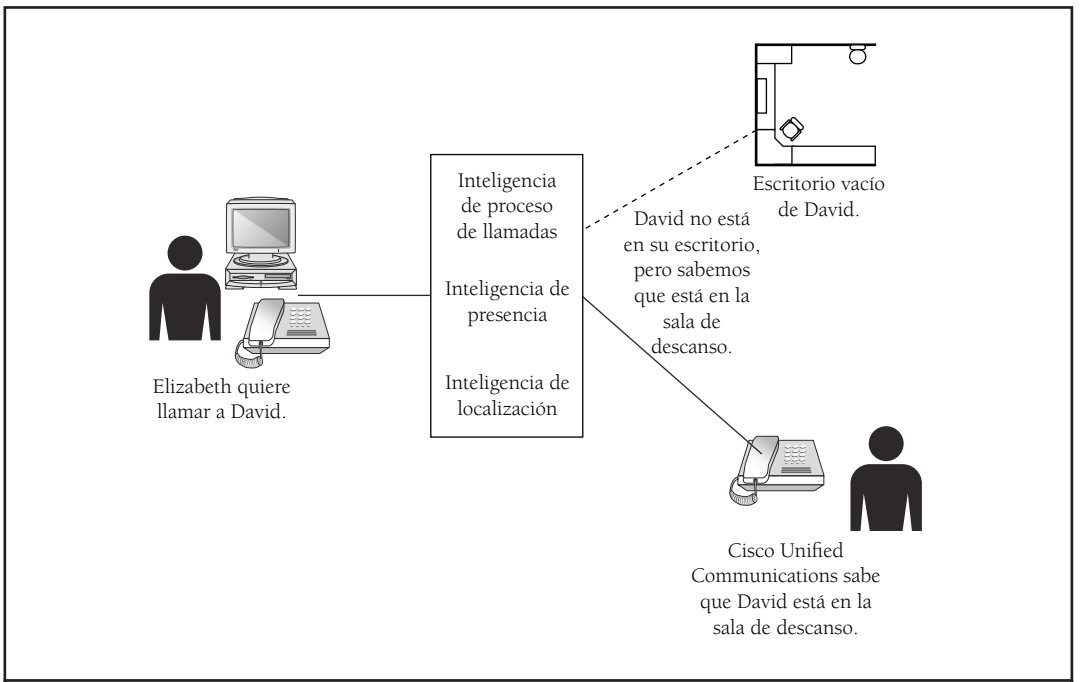


Figura 9-10. Cisco Unified Communications se basa en tres componentes.

enviar correos electrónicos a otras personas, de modo que se configuran cuentas de correo electrónico. No obstante, Cisco cree que faltan comunicaciones eficaces. En vez de sólo proporcionar un teléfono y una cuenta de correo electrónico, las comunicaciones necesitan ser más robustas e inteligentes.

Con la solución Cisco Unified Communications, los usuarios pueden hacer todo desde sus computadoras personales o teléfonos IP con un conjunto de aplicaciones ricas en características.

Cisco Unified Presence Server (servidor unificada de Cisco)

Una de las mayores atracciones del sistema Cisco Unified Communications es el Cisco Unified Presence Server. El servidor recolecta información acerca del estado de un usuario, incluido si él o ella está en el teléfono en ese momento, y luego las aplicaciones como el Cisco Unified Presence Server y el Cisco Unified CallManager (administrador de llamadas unificado de Cisco) pueden ayudar al usuario a conectarse al determinar la mejor manera de comunicación.

El servidor recaba información de la red junto con el Cisco Unified CallManager, equipos de terceros que utilizan SIP y SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE, SIP para mensajería instantánea y extensiones que impulsan la presencia), y luego publican esa información a Cisco Unified IP Phones (teléfonos IP unificado de Cisco), Cisco Personal Communicator (comunicador personal de Cisco) y aplicaciones de terceros, como Live Communications Server 2005 de Microsoft.

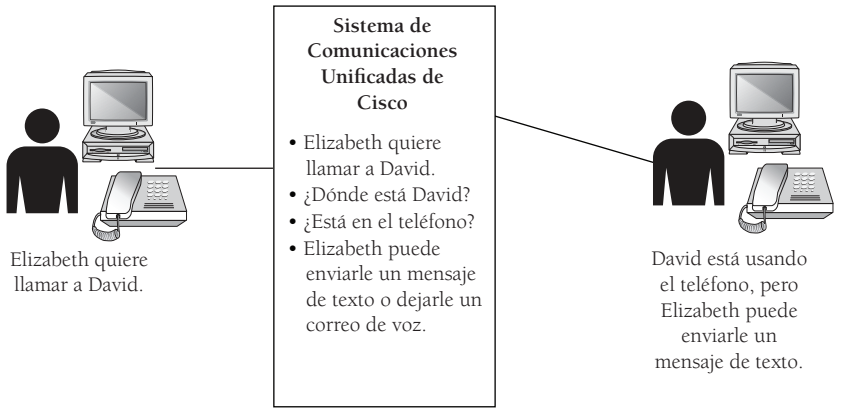


Figura 9-11. Cisco Unified Communications ayuda a conectar a los usuarios.

El proceso de comunicación con alguien que utiliza las Cisco Unified Communications se ilustra en la figura 9-11.

Soporte SIP

Por supuesto, la imagen global de Cisco Unified Communications es la convergencia. Cisco dio un gran paso cuando adoptó el protocolo SIP para comunicaciones en vez de impulsar el protocolo de su propiedad, SCCP, o delgado.

Como se mencionó antes, Cisco ha estado impulsando el protocolo SCCP desde hace varios años, pero debido a que era propiedad de Cisco, ningún equipo ni aplicaciones de terceros podían tomar parte de la solución de Cisco. Se trataba de una práctica de negocios que se proponía dar a Cisco el dominio en el mundo de la telefonía IP, en tanto las organizaciones decidieran dejar a sus otros proveedores para favorecer a Cisco.

La adopción de SIP es, tal vez, una mejor estrategia por parte de Cisco; permite que las aplicaciones y equipos de terceros formen parte de su estructura de comunicaciones unificadas. Aunque en algunos casos esto parecería un movimiento derrotista por parte de Cisco, en realidad hace que la disponibilidad de solución sea mucho mayor para las organizaciones. Además, por lo menos Cisco coloca un pie en la puerta.

Este cambio de filosofía es parte de Cisco Unified CallManager 5.0, una parte estratégica de la plataforma VoIP de Cisco. Este cambio permite a los teléfonos de otros proveedores comunicarse con CallManager, lo que antes no era posible. Naturalmente, esto permite a los clientes que poseen teléfonos habilitados para SIP aprovechar sus inversiones existentes. Una vez dicho esto, Cisco espera que los clientes se sientan más atraídos hacia sus teléfonos ricos en características cuando desarrollen una solución de telefonía IP.

Productos y componentes

Cuando se introdujo en marzo de 2006, Cisco Unified Communications incluía 40 productos diferentes para varias organizaciones y misiones. Esos nuevos productos, además de los equipos y aplicaciones existentes, pueden dividirse en cinco componentes:

- Telefonía IP.
- Aplicaciones de Cisco Unified Communications.
- Aplicaciones de Cisco Unified Contact Center (centro de contacto unificado de Cisco).
- Infraestructura de Cisco Unified Communications.
- *Suite* Cisco Unified Communications Management.

En las siguientes secciones se explican los productos de cada componente.

Telefonía IP

La telefonía IP, dentro de Cisco Unified Communications, incluye teléfonos individuales y aplicaciones de proceso de llamadas.

Teléfonos IP Aunque Cisco Unified Personal Communicators (comunicador personal unificado de Cisco) es una manera de hacerlo todo con una computadora, algunas personas quieren realmente utilizar un teléfono "a la antigüita". Cisco ofrece 14 modelos de Cisco Unified IP Phone en su serie 7900.

En la tabla 9-3 se comparan varios modelos dentro de dicha serie.

Producto	Número de líneas	Pantalla	Protocolos	Conmutador Ethernet
Cisco Unified IP Phone 7985G	1	Video	SCCP	10/100
Cisco Unified IP Phone 7971G-GE	8	Color	SCCP, SIP	10/100/1000
Cisco Unified IP Phone 7970G	8	Color	SCCP, SIP	10/100
Cisco Unified IP Phone 7961G-GE	6	Color	SCCP, SIP	10/100/1000
Cisco Unified IP Phone 7961G	6	Sí	SCCP, SIP	10/100
Cisco Unified IP Phone 7960G	6	Sí	SCCP, SIP, MGCP	10/100
Cisco Unified IP Phone 7941G-GE	2	Sí	SCCP, SIP	10/100/1000

Tabla 9-3. Comparación de los teléfonos unificados IP de Cisco (*continúa*).

Producto	Número de líneas	Pantalla	Protocolos	Conmutador Ethernet
Cisco Unified IP Phone 7941G	2	Sí	SCCP, SIP	10/100
Cisco Unified IP Phone 7940G	2	Sí	SCCP, SIP	10/100
Cisco Unified IP Conference Station 7936	1	Sí	SCCP	N/A
Cisco Unified IP Expansion Module 7914	14	Sí	N/A	N/A
Cisco Unified IP Phone 7912G	1	Sí	SCCP, SIP	10/100
Cisco Unified IP Phone 7911G	1	Sí	SCCP, SIP	10/100
Cisco Unified IP Phone 7905G	1	Sí	SCCP, SIP	No
Cisco Unified IP Phone 7902G	1	No	SCCP	No

Tabla 9-3. Comparación de los teléfonos unificados IP de Cisco (*conclusión*).

El Cisco Unified IP Phone 7985G es un teléfono con video (incluye cámara, pantalla, altavoz y auricular) todo en un solo aparato.

Cisco Unified Wireless IP Phone 7920 es un equipo 802.11b que se conecta a una red WiFi y proporciona los mismos tipos de presencia y características de comunicación que soportan sus demás hermanos alámbricos.

Cisco Unified Communications soporta teléfonos de modo dual a través de alianzas con Nokia y RIM. El cliente de teléfono de software de Cisco estará disponible en los teléfonos de modo dual, proporcionando acceso pleno a CallManager cuando se encuentran dentro de la red WiFi de la organización.

Procesamiento de llamadas Los diversos tipos de software de procesamiento de llamadas de Cisco se emplean para organizaciones de varios tamaños y tipos para manejar las llamadas de voz y video entre teléfonos IP, aplicaciones de proceso de medios de comunicación y gateways a la red telefónica conectada al sistema público.

En la tabla 9-4 se comparan los productos de proceso de llamadas de Cisco Unified Communications.

Producto	Número de usuarios	Distribuido o centralizado	Basado en servidor o enrutador
Cisco Unified CallManager	Hasta 30 000 por clúster	Centralizado	Servidor
Cisco Unified CallManager Express	Hasta 240	Centralizado para negocios pequeños, distribuido en sucursales	Enrutador
Cisco Unified Survivable Remote Site Telephony	Hasta 720	Distribuido en sucursales	Enrutador

Tabla 9-4. Productos de procesamiento de llamadas de Cisco Unified Communications.

Aplicaciones de Cisco Unified Communications

Aunque el término telefonía IP trae a la mente teléfonos especializados que se conectan a un puerto Ethernet, ésa no es la única forma de comunicación, en especial con la arquitectura de Cisco Unified Communications. Además, las funciones pueden emplearse en una computadora personal, sin tener que usar un teléfono especial. En esta sección se describen estos teléfonos de software, junto con otras aplicaciones relevantes.

Clientes Cisco ofrece tres aplicaciones de cliente de comunicaciones con varias características, desde funcionalidad de teléfono de software hasta telefonía de video. El producto de mayor nivel de Cisco en esta línea es el Comunicador Personal Unificado, que puede utilizarse en un entorno Windows o Mac.

El Cisco Unified Personal Communicator es una sola aplicación que maneja todas las comunicaciones del usuario: voz, video y datos. La herramienta tiene una GUI amigable con el usuario, lo que simplifica el desplazamiento entre múltiples aplicaciones. Al emplear la información de presencia dinámica, el usuario puede buscar en un directorio a la persona con la que quiere ponerse en contacto, hacer clic en ese registro y conectarse. Esto se simplifica aún más en el sentido de que emplea la información de la presencia para localizar a esa persona, sin importar el lugar de la organización en que esa persona se encuentre físicamente. Por ejemplo, si la persona no está en su lugar, la llamada podría dirigirse a su teléfono celular. En la tabla 9-5 se comparan estas aplicaciones.

Voz y mensajería La voz y la mensajería se entregan a organizaciones de diferentes tamaños y necesidades utilizando tres componentes de la familia Cisco Unified Communications. En la tabla 9-6 se comparan estos productos.

Producto	Aplicación de proceso de llamadas que se requiere	Capacidad de teléfono de software	Hardware adicional requerido
Cisco IP Communicator	Cisco Unified CallManager Express o Cisco Unified CallManager	Sí	Ninguno
Cisco Unified Video Advantage	Cisco Unified CallManager Express o Cisco Unified CallManager	No	Cisco VT Camera, Cisco Unified IP Phone
Cisco Unified Personal Communicator	Cisco Unified CallManager v5.0	Sí	Cisco Unified Presence Server

Tabla 9-5. Clientes de Cisco Unified Communications.

Conferencia en medios de comunicación Además, Cisco Unified Communications facilita en gran medida la conferencia de medios de comunicación. Si emplea Cisco Unified Personal Communicator, sólo haga clic en las personas a quienes quiere incluir en su llamada, y con eso los reúne en su llamada en conferencia. También podrá compartir medios de comunicación, colaborar y realizar una videoconferencia. Una vez más, Cisco tiene un producto para cada tamaño de organización.

En la tabla 9-7 se comparan los productos de conferencia de medios de comunicación.

Producto	Usuarios	Integración de correo electrónico	Conexión en red a otros sistemas de correo de voz	Integración con otros procesadores de llamada que no son de Cisco	Reconocimiento del habla
Cisco Unity Express	250	Integrado	Sólo Cisco Unity	No	No
Cisco Unity Connection	1 500	Integrado	No	Algunos	Sólo en inglés
Cisco Unity	7 500 por servidor; 250 000 en red	Integrado o unificado	Sí	Sí	Sí

Tabla 9-6. Componentes de voz y mensajes de Cisco Unified Communications.

Aplicaciones de Cisco Unified Contact Center (centro de contacto unificado de Cisco)

Las aplicaciones Cisco Unified Contact Center se emplean como parte de un centro de llamadas para mejorar las comunicaciones con los clientes. Existen varias aplicaciones que se pueden utilizar con base en una necesidad específica de la organización. Entre las aplicaciones se incluyen:

- **Cisco Unified Contact Center Express y Cisco Unified Contact Center Enterprise** Diseñada para organizaciones de todos los tamaños, esta solución simplifica la integración de aplicaciones, la administración de agentes y brinda enrutamiento de llamadas, administración de contactos, características de administración y de distribución automática de llamadas, entre las que se incluyen:
  - Enrutamiento condicional.
  - Cola de llamadas.
  - Mensajes de tiempo estimado de espera.
  - Informes a profundidad.
- **Portal de voz de Cisco Unified Customer** Los clientes utilizan esta aplicación para interactuar con el Cisco Unified Contact Center utilizando sólo la voz. Esta aplicación se basa en XML y se integra con el resto de una solución de Centro de Contacto Unificado de Cisco.

Producto	Usuarios concurrentes	Conectividad	Colaboración en red	Colaboración en video
Cisco Unified Meeting Place Express	20 - 120	IP	Sí	No
Cisco Unified Meeting Place	960 IP o 1 152 TDM	IP o TDM	Sí	Sí
Cisco Unified Video Conferencing	3 - 30	IP o ISDN	Colaboración de datos	Sí

Tabla 9-7. Productos de conferencia de medios de Cisco Unified Communications.

- **Customer Interaction Analyzer (analizador de interacción con los clientes)** Utilizada por el centro de contacto, esta tecnología puede escuchar una llamada y analizarla con base en la detección de palabras, el tono, la inflexión y la cadencia. Luego puede determinar el estado de ánimo del cliente y poner esa información analítica a disposición de otras aplicaciones. Esto puede pasarse al servicio al cliente para capacitación, de modo que puedan dar un mejor servicio la próxima vez.
- ▲ **Cisco Unified Intelligent Contact Management Enterprise (administración de contacto inteligente unificado de Cisco)** Una solución de enrutamiento de llamadas y telefonía en la computadora para los sistemas automáticos de distribución de llamadas de herencia. Esta solución puede tomar decisiones inteligentes de enrutamiento mientras la llamada está aún dentro del sistema de la red telefónica conectada al sistema público.

Infraestructura de comunicaciones unificadas de Cisco

Para funcionar de manera adecuada, las soluciones de Cisco Unified Communications requieren enrutadores y conmutadores específicos. Estos enrutadores y conmutadores incluyen:

- ▼ **Enrutadores** Series 2800, 3800 y 7200 de Cisco.
- ▲ **Conmutadores** Series 2560, 3570, 4500 y 6500 de Cisco Catalyst y la serie 500 de Cisco Catalyst Express.

Suite Cisco Unified Communications Management

Cisco Unified Operations Manager (administrador de operaciones unificadas de Cisco) y Cisco Unified Services Monitor (monitor de servicios unificados de Cisco) se emplean para administrar las soluciones de Cisco Unified Communications:

- ▼ **Cisco Unified Operations Manager** Proporciona una sola visión de todo el despliegue de Cisco Unified Communications. Da el estado operacional de cada componente en la solución y vigila ese estado.
- ▲ **Cisco Unified Services Monitor** Vigila las celdas activas y notifica si la calidad de la voz cae por debajo de los parámetros establecidos por el administrador de la red.

En realidad, VoIP nunca fue la máxima aplicación en Internet, pero está adquiriendo importancia con rapidez. Aunque las primeras presencias fueron buenas formas de ahorrar algo de dinero, en especial en la comunicación con las sucursales, el campo adquiere cada vez más riqueza en características. Hoy en día, VoIP ofrece a las organizaciones nuevas y apasionantes formas de comunicarse dentro de la organización, así como a quienes llaman a ésta.

CAPÍTULO 10

Herramientas de almacenamiento

En el capítulo anterior, dijimos que la amalgama de voz y datos en un solo circuito es una meta para muchas organizaciones de interconexiones. A medida que aumenta el tráfico a través de la red, la demanda de almacenamiento será creciente. Por desgracia, los medios convencionales de almacenamiento de datos (conjuntos de discos y copias de seguridad de cintas conectadas al servidor) no son suficientes para seguir con la tarea.

Además, junto con el lema "la era de la información" viene la responsabilidad de almacenar datos de todos tipos de tamaño y composiciones. No sería malo que el término "información" se limitara a páginas de palabras escritas, con las ocasionales fotografías. No obstante, en años recientes, la "información" ha evolucionado a un rico contenido multimedia, que mezcla imágenes y sonidos. Estos archivos gráficos y de sonido son cada vez más grandes y poseen mayores detalles, lo que significa archivos de mayor tamaño. Además, las organizaciones ya no se limitan a almacenar los datos para archivarlos. Se accede a esta información de manera rutinaria en forma interna o por medio de un sitio Web para los visitantes. Por ejemplo, observe la proliferación de programas de televisión, películas y música que es posible poner en línea y descargar a la computadora o el equipo multimedia de un consumidor. La buena noticia es que hay más multimedia en el horizonte. La mala noticia es las organizaciones que manejan este tipo de contenidos deben encontrar una manera de almacenarla y manejarla con la mayor eficiencia que les sea posible.

Tan maravillosa como es la multimedia, las necesidades de almacenamiento de estos archivos tienen un costo. El equipo convencional de almacenamiento en red es cada vez más incapaz de mantener toda esta información. Por si esto fuera poco, la transferencia de grandes cantidades de datos crea sus propios problemas, en tanto que el ancho de banda de las redes se ve cada vez más exigido por otras cargas.

Después de dos décadas, el bus paralelo Small Computer System Interface (SCSI, interfaz de sistema de computadora pequeña) que facilitó la conectividad entre servidores de almacenamiento para los servidores LAN, impone límites al almacenamiento en red. Aunque las conexiones SCSI son adecuadas para las computadoras personales y las LAN, no son lo bastante robustas para las necesidades de almacenamiento a gran escala. Aumentando las limitaciones de SCSI se encuentra el uso tradicional de las conexiones LAN para respaldo de almacenamiento de servidores, lo que requiere ancho de banda útil del cliente.

Cuando se trata del almacenamiento masivo, las organizaciones disponen de un par de opciones populares, que son:

- **Direct Attached Storage (DAS, almacenamiento adjunto directo)** Con esta opción, los datos activos de una organización se mantienen en discos conectados a los servidores de cómputo. Sin embargo, esto es un desperdicio cuando la empresa tiene varios servidores que operan diferentes aplicaciones, porque DAS se vuelve ineficiente: algunas de las unidades de almacenamiento se quedan sin espacio, en tanto que otros disponen de grandes cantidades de espacio no utilizado.
- **Network-Attached Storage (NAS, almacenamiento adjunto de red)** Con esta opción, las organizaciones remueven los sistemas de almacenamiento de los servidores, para usar mejor el espacio y hacer más modulares las redes, lo que simplifica las reparaciones y las actualizaciones. Por ejemplo, una solución NAS supone una unidad de disco con un hardware que pone el sistema de archivos disponible en una red IP. Los datos se reúnen en un solo lugar. Esto hace más rápido respaldar, archivar y recuperar, lo que es ideal para algunos escenarios, pero el desempe-

ño de NAS se rige por la velocidad de la red y los protocolos específicos. Al final de este capítulo analizaremos algunas soluciones NAS.

- **Storage Area Network (SAN, red de área de almacenamiento)** Se trata de una opción más compleja y poderosa de almacenamiento. Las SAN conectan a los servidores y almacenan en sus propias redes.

En este capítulo, hablaremos primero de las generalidades de SAN y de la forma en que puede diseñar una SAN para sus propias necesidades de trabajo en red. Después trataremos las soluciones SAN de Cisco.

REDES DE ÁREA DE ALMACENAMIENTO

Una solución al problema de la escasez de almacenamiento consiste en implantar una SAN. Las SAN son redes que se diseñan, construyen y mantienen con un propósito: almacenar y transferir datos. Las SAN son un campo en auge, y se espera que logren un impresionante crecimiento.

Necesidades de almacenamiento

Con la popularidad de Internet y el aumento masivo del comercio electrónico, las organizaciones buscan un medio para almacenar grandes cantidades de datos. Una forma popular de mantener terabytes de información emplea SAN, que interconecta dispositivos de almacenamiento con conmutadores Fibre Channel. Si bien el almacenamiento de datos es barato (es posible adquirir un disco duro de 200 GB por un par de cientos de dólares) esto es una respuesta reactiva a la escasez de almacenamiento. Al crear un remiendo de discos duros, los gastos generales de la red de Internet se disparan y lentamente pierde el control.

Por otro lado, las SAN permiten manejar todas las necesidades de almacenamiento de una forma proactiva al tiempo que se mantiene la alta disponibilidad que se requiere. En la figura 10-1 se ilustra un ejemplo de la forma en que LAN y SAN funcionan de manera conjunta.

En la medida que las organizaciones y sus necesidades de cómputo crecen, también lo hace su dependencia del almacenamiento de datos. Por ejemplo, cada vez que más empresas agregan conjuntos de servidores para manejar sus asuntos internos y externos, más confiable debe ser la interconexión. Para garantizar una alta disponibilidad, los servidores que comparten grupos de almacenamiento en una SAN pueden transferirse a un sistema secundario sin mayor dificultad en el servicio. Además, debido a que la fibra óptica es la espina dorsal de las SAN, la recuperación de desastres disminuye de varias horas a algunos minutos, o menos.

Al combinar los modelos de redes LAN con los bloques fundamentales de construcción del desempeño de servidores y la capacidad de almacenamiento masivo, las SAN eliminan los cuellos de botella de ancho de banda y las limitaciones de escalabilidad que imponían las arquitecturas anteriores basadas en bus de SCSI. Además de los beneficios fundamentales de la conectividad SAN, las nuevas capacidades facilitadas por el enfoque de red SAN, elevan su valor como infraestructura de largo plazo. Estas capacidades, que incluyen agrupamiento, flexibilidad topológica, tolerancia a las fallas, alta disponibilidad y administración remota, elevan aún más la capacidad de SAN para abordar los crecientes retos de las aplicaciones intensivas en datos, que son críticas para la misión.

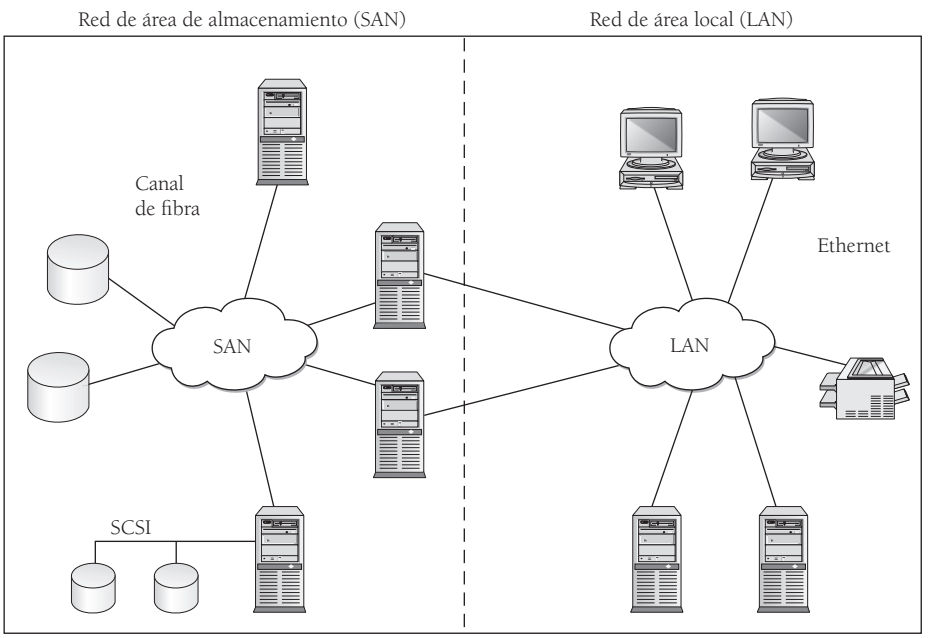


Figura 10-1. Las SAN y LAN operan de manera independiente, pero pueden unirse entre sí.

Existen tres componentes primarios de la red de área de almacenamiento:

- ▼ **Interfaz** La interfaz es lo que permite que el almacenamiento sea externo al servidor y la agrupación de los servidores. SCSI, Fibre Channel (canal de fibra), iSCSI y Fibre Channel Over IP (FCIP, canal de fibra sobre IP) son interfaces comunes SAN.
- ■ **Interconectar** Interconectar es el mecanismo que emplean estos dispositivos para intercambiar datos. Se emplean dispositivos como concentradores, enrutadores, gateways y conmutadores para vincular varias interfaces a la red SAN.
- ▲ **Retícula** La plataforma (combinación de protocolo y topología de red) se basa en SCSI conmutado, fibra conmutada, etcétera. El uso de las gateways permite extender la SAN a lo largo de WAN.

Fibre Channel

Fibre Channel es una interfaz serial de alta velocidad y estándar de la industria para conectar las computadoras personales y los sistemas de almacenamiento. Fibre Channel permite juntar servidores y sistemas de almacenamiento en distancias de hasta 100 kilómetros (que es casi 4 000 veces más lejos que las interfaces paralelas SCSI). Esto permite colocar las instalaciones de almacenamiento en otro piso, en otro edificio o incluso en otra ciudad.

Fibre Channel posee 200 veces más ancho de banda que SCSI (4 Gbps contra 20 Mbps). Además, Fibre Channel soporta varios protocolos estándar (como TCP/IP y SCSI) de manera concurrente sobre el mismo cable físico. Es útil porque simplifica el cableado y mantiene bajos los costos de infraestructura. Debido a que Fibre Channel permite transportar los paquetes estándar SCSI a través de líneas de fibra óptica, es posible mantener y utilizar los dispositivos SCSI existentes junto con los dispositivos Fibre Channel.

NOTA Aunque Fibre Channel se utiliza con mayor frecuencia con conexiones de fibra óptica, es posible utilizarlo con cableado de cobre. Sin embargo, los cables de cobre imponen mayores limitaciones de velocidad y distancia que la fibra óptica. Además, el cobre puede sufrir degradación del desempeño debido a la interferencia electromagnética.

Por consideración a la confiabilidad a través de la abundancia, las SAN de Fibre Channel deben construirse en torno de concentradores y conmutadores SAN. Esto garantiza que no exista ningún punto de falla y que se mejore el desempeño de los cuellos de botella. Quizá esto suene conocido, porque es una consideración fundamental cuando se diseña una LAN.

Capas de Fibre Channel

El estándar Fibre Channel contiene cinco capas. Cada una de ellas es responsable de un conjunto específico de funciones. Si recuerda por un momento el capítulo 2, observará algunas características comunes entre Fibre Channel y el modelo OSI. En el modelo Fibre Channel, las capas se numeran FC-0 a FC-4.

En la tabla 10-1 se describen las diferentes capas del modelo Fibre Channel, y en la figura 10-2 se ilustra este apilamiento.

Aunque los apilamientos de datos son diferentes (sobre todo porque el modelo OSI tiene siete capas, y Fibre Channel sólo tiene cinco), cada capa en el modelo depende de la capa que está inmediatamente debajo o encima de ella.

Debido a que Fibre Channel utiliza el formato de capas, los productos y aplicaciones que funcionan en una capa son compatibles con los que residen en otra capa, que es lo que hace el modelo OSI.

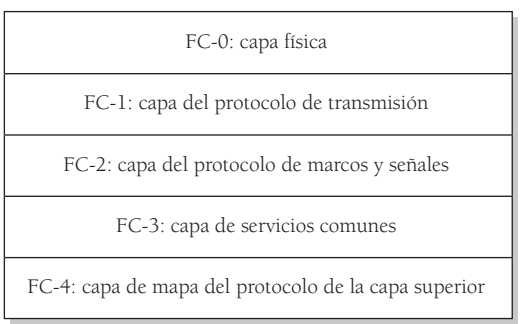


Figura 10-2. La pila de Fibre Channel contiene cinco capas.

Capa	Descripción
FC-0: capa física	Define el cableado, los conectores y las señales que controlan los datos. Esta capa es similar a la capa física OSI.
FC-1: capa del protocolo de transmisión	Responsable de la detección de errores, mantenimiento de vínculos y sincronización de datos.
FC-2: capa del protocolo de marcos y señales	Responsable de la segmentación y el reensamblaje de paquetes de datos que el equipo envía y recibe. Además, en esta capa se realizan la secuenciación y el control de flujo.
FC-3: capa de servicios comunes	Proporciona servicios como transmisión múltiple y segmentación de datos de secuencia lógica.
FC-4: capa de mapa del protocolo de la capa superior	Proporciona el punto de comunicación entre los protocolos de la capa superior (como SCSI) y las capas inferiores de Fibre Channel. Esta capa permite que más datos SCSI recorran el vínculo Fibre Channel.

Tabla 10-1. Capas en la pila de Fibre Channel.

Recorrido de la distancia

Las soluciones de almacenamiento SCSI deben ubicarse junto al servidor porque su rango está limitado a 25 metros. Esto es un problema, sobre todo si no hay espacio en la sala de servidores. Debido a que Fibre Channel permite ubicaciones a larga distancia entre los servidores y el equipo de almacenamiento, las dos piezas del equipo pueden estar hasta a 100 kilómetros.

Es posible agregar tres tecnologías a los dispositivos SAN de Cisco para proporcionar conectividad Fibre Channel. Estas tecnologías emplean distintas longitudes de onda láser para recolectar diversos niveles de ancho de banda y distancia. Estas longitudes de onda son:

- ▼ **Short WaveLength (SWL, longitud de onda corta)** Proporciona conectividad hasta 500 metros.
- ■ **Long WaveLength (LWL, longitud de onda larga)** Proporciona conectividad hasta 10 kilómetros.
- ▲ **Coarse WaveLength Division Multiplexing (CWDM, multiplexaje de división de longitud de onda amplia)** Proporciona conectividad hasta 100 kilómetros.

Sin embargo, en la práctica, la capacidad de los datos de recorrer grandes distancias puede ser útil si se construye un centro de almacenamiento para mantener todos los datos para varios departamentos. Además, varios servidores que se ubican en un campus podrían

enviar sus datos a una instalación de almacenamiento central que se encuentra en un edificio separado. Esto permite la creación de grupos modulares y escalables de almacenamiento.

Aumento en la conectividad

El uso de Fibre Channel también simplifica la conectividad de sistemas múltiples con acceso a un equipo de almacenamiento compartido al superar las limitaciones de la SCSI paralela, incluida la distancia y el número de dispositivos por bus. Fibre Channel soporta ocho veces más equipos por ciclo que la SCSI paralela. No obstante, en la práctica quizá no sea realista poner tantos equipos en el mismo ciclo. Sin embargo, hoy en día existe la capacidad para que grandes números de servidores tengan acceso a los equipos de almacenamiento como arreglos RAID o bibliotecas de cintas.

Otros protocolos SAN

Además de Fibre Channel, existe un par de protocolos SAN que hay que tomar en cuenta. Estos protocolos son útiles en el diseño y despliegue de SAN óptimas y pueden utilizarse como parte de su solución SAN. Hablemos de los dos protocolos que hoy en día predominan (FCIP e iSCSI) y frotemos nuestra bola de cristal para ver el futuro del protocolo iFCP de SAN.

iSCSI

El primer protocolo es la canasta en que, hace algunos años, Cisco pareció poner todos sus huevos (interfaz de sistema de computadora pequeña sobre IP). En esencia, sólo son datos transportados en el protocolo SCSI sobre redes TCP/IP. SCSI es el lenguaje de los discos duros, e iSCSI es un protocolo que encapsula los comandos SCSI y los datos de transporte a través de redes IP. Es benéfico, porque interopera con las aplicaciones y sistemas operativos existentes, así como con redes de tipo LAN y WAN.

Los productos que utilizan iSCSI permiten que los hosts en una red IP se conecten a través de las redes Gigabit Ethernet a Fibre Channel o a un almacenamiento SCSI. Las redes de almacenamiento IP se construyen de manera directa sobre las redes existentes. Esto no salió del modo que Cisco había esperado, pero no quiere decir que iSCSI sea una tecnología muerta. Sigue siendo un protocolo viable y se emplea en muchos de los equipos SAN de Cisco (y de otros proveedores). De hecho, iSCSI y Fibre Channel son predominantes en los despliegues SAN.

FCIP

Un protocolo más reciente es FCIP, o Fibre Channel sobre IP (canal de fibra sobre IP). FCIP representa dos tecnologías distintas fusionadas (redes de almacenamiento y de larga distancia). FCIP combina los mejores atributos de Fibre Channel y del protocolo Internet para conectar SAN distribuidas. FCIP encapsula Fibre Channel y lo envía por un conector TCP.

Se considera que FCIP es un protocolo de túnel debido a que hace una conexión transparente punto a punto entre SAN separadas geográficamente, utilizando redes IP. FCIP depende de los servicios TCP/IP en cuanto a conectividad entre SAN sobre LAN, MAN y WAN. Además, TCP/IP tiene la tarea de administración y control de congestión, así como de los errores de datos y recuperación de éstos. El beneficio es que las organizaciones pueden aprovechar sus inversiones existentes en tecnología extendiendo la red de Fibre Channel sobre un vínculo IP.

iFCP

Además, para confundir las cosas con FCIP, otro protocolo SAN es iFCP (Internet Fibre Channel Protocol, protocolo Fibre Channel de Internet). Aunque las letras son las mismas (pero en un orden diferente, para realmente confundir las cosas), la tecnología es muy diferente. iFCP permite a una organización extender Fibre Channel en Internet utilizando TCP/IP. Esto suena muy similar a FCIP, pero allí es donde terminan las similitudes. Aunque FCIP se emplea para extender una retícula Fibre Channel con un túnel con base en IP, iFCP está un movimiento más lejos de las SAN actuales de Fibre Channel hacia el futuro de las SAN de IP.

Las gateways iFCP pueden complementar las retículas existentes de Fibre Channel, o bien suplantarlas por completo. iFCP permite a las organizaciones crear una retícula SAN de IP, reduciendo al mínimo el componente Fibre Channel y aumentando al máximo el uso de la infraestructura TCP/IP.

Aunque la solución de Cisco, de la que hablaremos en la siguiente sección, se basa en gran medida en FCIP, es útil saber qué hay en el horizonte con iFCP.

Diseño y construcción de una SAN

Cuando se trata de diseñar y construir una SAN, es necesario considerar varios factores importantes antes de conectar la fibra a los enrutadores y conmutadores. Se deben considerar cuestiones como el tipo de aplicaciones que se utilizarán, el mejor diseño para la espina dorsal, cómo se configurará la topología y qué mecanismos se emplearán para manejar la SAN. Observemos más de cerca cada uno de estos temas.

Necesidades de aplicación

Al desarrollar y diseñar una SAN, el primer paso es determinar a qué aplicaciones servirá. Sin importar si se diseña un conjunto de datos comunes para un banco de servidores Web, una red de flujo de datos de alto desempeño o para cualquier otra necesidad, es preciso prestar especial atención a la infraestructura SAN. Es necesario tomar en cuenta cuestiones como las densidades de puerto, distancia y requerimientos de ancho de banda, y segmentación. Todas estas variables se ven afectadas por la aplicación.

NOTA En un entorno mixto, es importante evaluar las plataformas que compondrán la SAN. El soporte de hardware y software para SAN es variable, dependiendo de las plataformas que se empleen. Una vez que se hayan resuelto estas preguntas fundamentales, se podrá comenzar a construir la SAN.

La construcción de una SAN es similar a una infraestructura típica de Ethernet. Una SAN abarca algunos componentes básicos: el almacenamiento en discos de Fibre Channel y bibliotecas de cinta, concentradores y conmutadores de fibra, Host Bus Adapters (HBA, adaptadores de bus del host), y alguna forma de administración SAN.

Espina dorsal

A medida que se diseña la SAN, utilizar un ciclo arbitrado o una retícula conmutada es una decisión crítica de la arquitectura de hardware:

- ▼ **Ciclo arbitrado** Comparte el ancho de banda y emplea el envío general de datos. En cierto tiempo, fue la única opción para las columnas vertebrales SAN.
- ▲ **Retícula conmutada** Dedica el ancho de banda completo a cada puerto y permite transferencias simultáneas de datos a un solo nodo.

Su elección se decidirá en gran medida con base en sus necesidades de escalamiento y su desempeño. Si sus necesidades de almacenamiento son modestas, un simple concentrador debe ser suficiente para satisfacer sus necesidades. En el otro extremo del espectro, los grandes entornos de almacenamiento casi exigen los conmutadores de fibra.

En los grupos pequeños o las pequeñas oficinas/oficinas en casa, una buena base es un concentrador Fibre Channel en una configuración de ciclo arbitrado. Los concentradores son idóneos para estos entornos debido a que proporcionan un alto nivel de interoperabilidad a un precio razonablemente bajo. Los concentradores soportan un ancho de banda agregado de 100 Mbps. Los concentradores pueden soportar hasta 127 equipos, pero para resultados óptimos, se deberán limitar a 30 equipos. Además, debido a que los costos por puerto de un conmutador son más elevados que los de un concentrador, el concentrador es mejor para eliminar los puertos básicos de conmutadores a los servidores conectores.

Una de las principales razones por las que los concentradores están limitados en su estabilidad se debe a la forma en que los equipos se agregan al ciclo. Con el propósito de reconocer los demás equipos en dicho ciclo, cada uno de ellos debe realizar un *Loop Initialization Sequencer* (*LIP, secuenciador de inicialización de ciclo*) cuando se une por primera vez a la red. Cuando se realiza esta acción, el ciclo se suspende al tiempo que los demás miembros del mismo adquieren o verifican las direcciones de puerto, y se asigna una *dirección física de ciclo arbitrado.* Si bien el proceso de reconocimiento es bastante rápido, el tráfico sensible al tiempo (como VoIP o las copias de seguridad de datos) pueden verse afectados de manera negativa por estos limitadores de la velocidad del desempeño.

Por otro lado, los concentradores son útiles porque son baratos y fáciles de configurar, e interoperan bien con otros concentradores y productos de otros proveedores.

Fibra

Si las SAN son tan fantásticas, ¿por qué hasta ahora escuchamos de ellas? El principal factor que puso en juego las SAN como tecnología viable es el uso de fibra conmutada.

Los conmutadores de fibra soportan hasta 4 Gbps full-duplex en todos los puertos. A diferencia de los concentradores que, como se dijo antes, requieren un LIP, un conmutador de fibra necesita que los nodos conectados a sus puertos realicen un acceso *a la red.* El conmutador es el único dispositivo que ve este acceso, lo que permite que los dispositivos entren y salgan de la red sin interrumpir a los demás dispositivos.

Los dispositivos en un concentrador de ciclo arbitrado, que cae en cascada desde un conmutador, no son fundamentalmente compatibles con los demás dispositivos de la retícula. A diferencia de un entorno LAN conmutado, los equipos en un entorno SAN conmutado deben acceder en la red para poder comunicarse con los demás equipos. Sin embargo, los dispositivos que no cuentan con soporte de red por lo general son incapaces de operar en éstas, porque no realizan un acceso en la red. Más bien, emplean un LIP.

Configuración

Al igual que en una LAN, existen varias formas de configurar los conmutadores, proporcionando diferentes niveles de desempeño y redundancia. En una SAN, el diseño básico

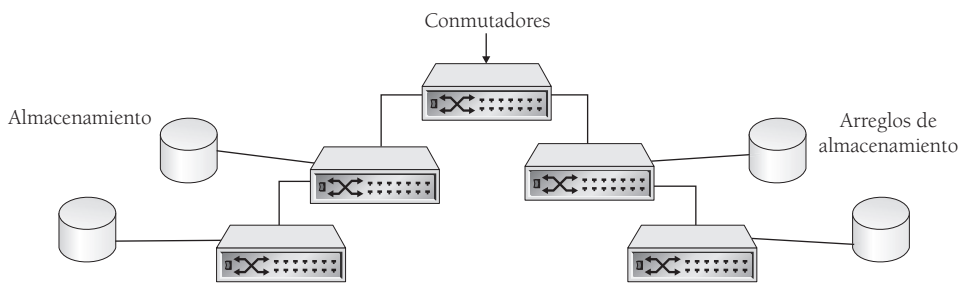


Figura 10-3. El modelo de árbol es la topología básica de una SAN.

de la configuración es el modelo de tipo árbol. En este esquema, los conmutadores caen en cascada entre sí y se dispersan por la SAN, como se ilustra en la figura 10-3.

El principal problema de este modelo son las limitaciones de escalabilidad debido a la latencia implícita en una interfaz de puerto único. Esto también limita el ancho de banda y no es ideal porque puede ser un solo punto de falla. Este tipo de diseño es mejor como una alternativa a los concentradores de fibra para una SAN que tiene una cascada de un solo nivel.

Para SAN más grandes e intrincadas, la mejor opción, tanto para una alta disponibilidad como desempeño es el modelo de malla. Ésta hace una gran red de conmutadores: cada concentrador está conectado a todos los demás, eliminando así la oportunidad de un solo punto de falla. Asimismo, la malla reduce los cuellos de botella y la latencia. El modelo de malla se ilustra en la figura 10-4.

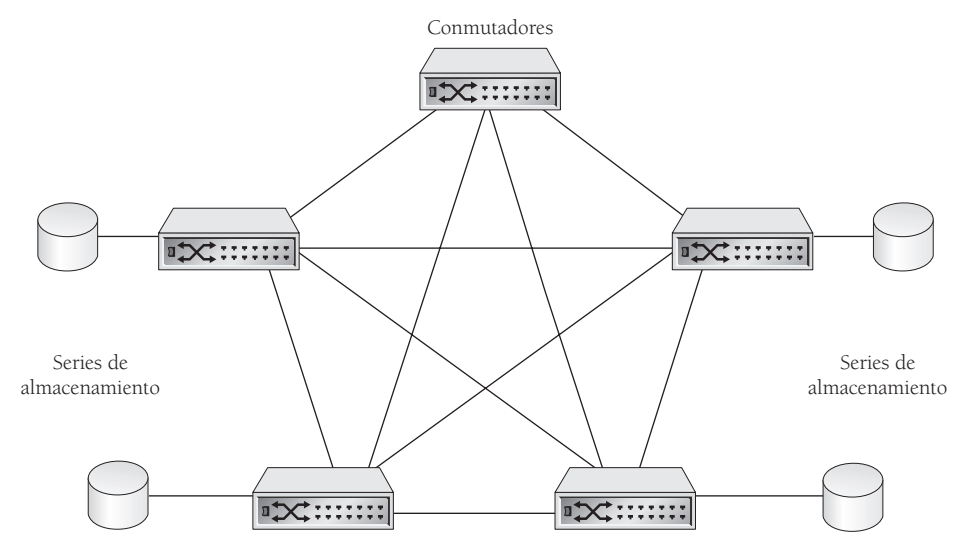


Figura 10-4. Una malla elimina cuellos de botella y puntos únicos de falla.

Una malla no es perfecta. El mayor problema es que no se escala de manera muy eficiente. Como se puede decir, mientras más conmutadores se agreguen, el número de puertos necesarios para conectar a todos los conmutadores disponibles emplearán la mayoría de los puertos en cada uno de los conmutadores. Dada esa limitación, la fortaleza de la malla es una buena opción para SAN de tamaño medio con cinco o menos conmutadores que requieren un tiempo máximo garantizado de operación y un desempeño óptimo.

La escalabilidad y la redundancia se integran en el siguiente modelo, como se muestra en la figura 10-5. A fin de asegurar una trayectoria redundante de datos, cada conmutador se conecta a otros dos. Así, cada conmutador tiene dos caminos diferentes a través de SAN, eliminando con ello un solo punto de falla. Esta configuración es una solución ideal para una SAN de clase empresarial.

Administración

Para que una SAN trabaje a su máximo, debe emplear dispositivos administrados centralmente. La administración SAN es sobre todo un dispositivo de seguridad que asegura que los servidores sólo vean los servicios destinados y las series de almacenamiento, reduciendo la posibilidad de corrupción de datos. Existen dos modos básicos de administrar el hardware de SAN: zonificación en el nivel de puerto y zonificación a Logical UNit (LUN, nivel de unidad lógica).

- La *zonificación en el nivel de puerto* es similar a una LAN virtual (VLAN). Los dispositivos de las particiones de la zonificación se basan en qué puertos se emplean en el concentrador o conmutador. Los nodos anexos no podrán comunicarse a menos que los puertos individuales se compartan en una zona común.

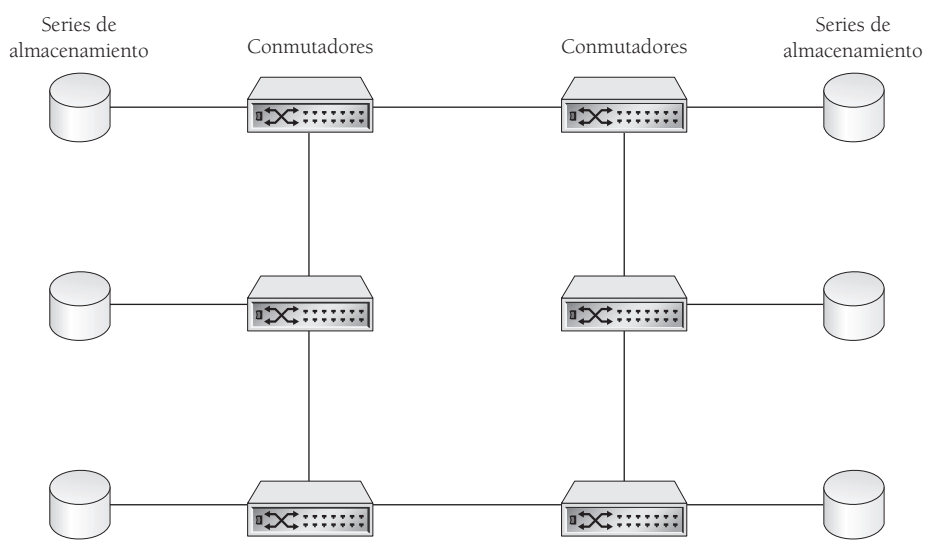


Figura 10-5. La conexión de otros dos dispositivos reduce los cuellos de botella y eleva la escalabilidad.

- La *zonificación en el nivel de unidad lógica* es similar a la de nivel de puertos; sin embargo, aumenta la especificidad, con lo que hace posible dividir los nodos con base en la identificación del dispositivo. La zonificación a nivel LUN da mayor flexibilidad cuando se trata de comunicarse con los equipos en el límite de la SAN.

NOTA Hablaremos más de la zonificación con equipos Cisco más adelante en este capítulo e incluiremos un análisis de SAN virtuales (VSAN).

El almacenamiento de datos puede ser un entorno en cambio permanente. Las necesidades de almacenamiento pueden diferir de manera drástica de un día al otro. Sin embargo, por fortuna, la administración de una SAN es útil, porque proporciona la capacidad de asignar de manera dinámica el almacenamiento a los diferentes grupos sin tener que reinicializar los servidores en el clúster de almacenamiento. Además, es posible agregar más almacenamiento al SAN y reasignarlo como se desee, una vez más sin interrupción.

Opciones de almacenamiento

Cuando se trata de decidir lo que se utilizará como el componente de almacenamiento de la SAN, no hay muchas opciones. Una sencilla, en especial si ya se cuenta con SCSI RAID o gavetas de discos, consiste en comprar un puente de SCSI a fibra. Un puente le permitirá conectar casi cualquier dispositivo SCSI a la SAN. El inconveniente es que se pierde toda la velocidad que proporcionaría un dispositivo anexo de manera original. Los puentes impulsan entre 15 y 40 Mbps.

Esto nos lleva a la segunda opción: almacenamiento original anexo a fibra. El almacenamiento de Fibre Channel es cada vez más popular y (como ocurre con la tecnología) el precio tiende a disminuir. El almacenamiento en fibra puede impulsar 4 Gbps, pero si bien los precios están bajando, no son tan baratos como la solución SCSI RAID. En cuanto a costos, los discos duros están a la par con los discos SCSI. Son los controladores externos Fibre Channel RAID que cuestan entre 8 000 y 50 000 dólares los que elevan el precio.

Copia de seguridad

Las copias de seguridad de fibra óptica son precisamente lo que necesitan los administradores que manejan redes con grandes cantidades de datos. No sólo pueden descargar las copias de seguridad de la red, sino que asimismo pueden compartir una sola biblioteca entre varios servidores dispersos en varios departamentos. Además, los recursos pueden asignarse a los departamentos que tienen las mayores necesidades de copias de seguridad. Además de los discos, las bibliotecas de cinta pueden emplear puentes SCSI a fibra. Aunque las bibliotecas de cinta no se acercan a la velocidad de los discos y pueden parecer un desperdicio de recursos de fibra, muchos instrumentan bibliotecas de cinta en sus SAN, porque las copias de seguridad son más fáciles de realizar.

Los enrutadores comienzan a entrar por sí mismos al mundo de las SAN. Los enrutadores en una SAN son dispositivos inteligentes capaces de ejecutar una copia de seguridad en forma directa de disco a cinta sin que el servidor intermediario procese primero la información. Como es posible imaginar, respaldar la información sin cargar al servidor no sólo libera a éste para realizar otras tareas, sino que también reduce los tiempos de copia de seguridad al retirar cualquier cuello de botella que pudiera ocurrir a la medida que los datos se filtran por el servidor. Además, los enrutadores poseen la tecnología integrada en

ellos para manejar la recuperación de errores, así como la capacidad de reportar problemas al software de copia de seguridad.

CONMUTADORES Y DIRECTORES CISCO MDS

La solución SAN de Cisco es Multilayer DataCenter Switches (MDS, conmutadores de centros de datos de capas múltiples). Los dispositivos MDS que se introdujeron en el 2003, son la entrada de Cisco al mundo de SAN y de su administración. Pero Cisco no sólo ha desarrollado su propia línea de equipos, sino que la empresa también ha integrado nuevas e interesantes herramientas, tecnologías y software. En esta sección, primero miraremos con más detalle las tecnologías que se encuentran detrás de la solución de Cisco. Luego, veremos el hardware específico que Cisco ofrece para la conmutación SAN. Por último, no es posible ensamblar todos estos equipos y esperar que funcionen (Cisco ofrece un par de paquetes de software para facilitar la configuración y la administración SAN).

Tecnologías

Además de las herramientas fundamentales que funcionan en las SAN que analizamos en la sección anterior, Cisco agrega algunas otras tecnologías a su solución SAN. Si bien algunas filosofías son comunes con las SAN de otros proveedores, Cisco incorpora algunas ideas nuevas, como SAN virtual, truncamiento y su propia versión de la seguridad SAN. Analicemos estas tecnologías con mayor detalle.

VSAN

Piense de nuevo en el capítulo 5 y en el análisis de las LAN virtuales. El mismo tipo de lógica se encuentra en operación detrás de las SAN virtuales (VSAN) y zonas.

Las VSAN (que comenzaron como tecnología propiedad de Cisco y desde entonces se han vuelto un estándar de la industria) permiten que las retículas independientes y lógicas se definan desde un conjunto de uno o más conmutadores. Las VSAN se aíslan de otras VSAN y funcionan como una retícula separada e independiente, con su conjunto propio de servicios, como asignación de nombre, zona, ruta, etcétera.

Con el propósito de transferir el tráfico de datos entre dos o más VSAN, la línea MDS de Cisco emplea la técnica llamada *enrutamiento inter-VSAN.* Éste permite la transferencia de datos entre fuentes y destinos en diferentes VSAN, como se muestra en la figura 10-6, pero sin comprometerlos al fusionarlos en una sola retícula. Esto asegura poder compartir los datos entre diferentes VSAN, pero sin afectar la escalabilidad, confiabilidad y seguridad de éstos.

Además, el enrutamiento inter-VSAN funciona a través de WAN utilizando FCIP. Esto permite emplear las características de enrutamiento a través de largas distancias, lo cual es ideal para las organizaciones cuyos activos están dispersos en diversos lugares.

La capacidad para conectar VSAN a través de un vínculo WAN es útil, porque es posible interconectar las retículas aisladas en los centros remotos de datos. Además, las VSAN suplementan la escalabilidad de los conmutadores y la creación de varias “islas” SAN, que eliminan la necesidad de un conmutador separado para diferentes aplicaciones.

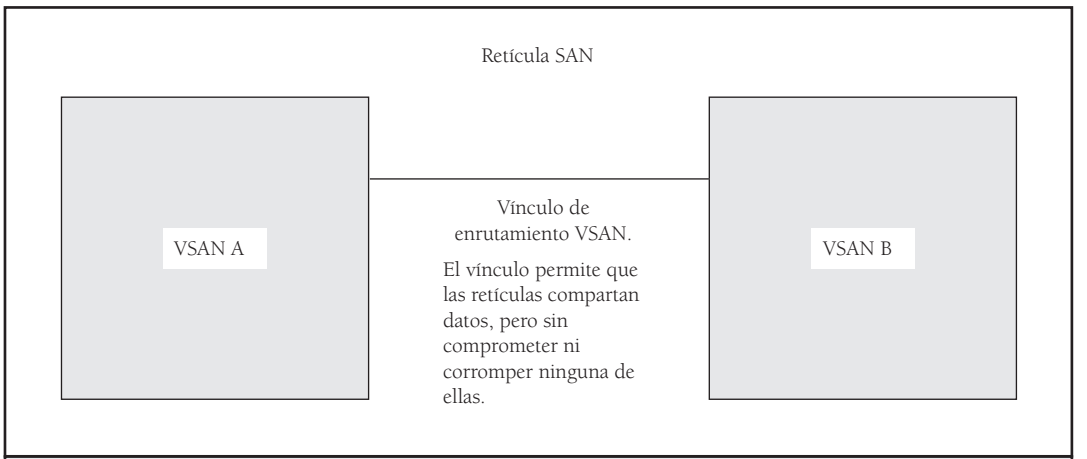


Figura 10-6. El enrutamiento inter-VSAN permite transferir los datos sin comprometerlos entre diferentes VSAN.

Zonificación

La zonificación es otro método que permite limitaciones en el acceso de los usuarios a los dispositivos de almacenamiento. Si bien todos los usuarios, de forma técnica, tienen acceso a los mismos dispositivos, sólo se les otorga permiso para utilizar partes de dispositivos específicos. En este caso, el beneficio debe ser obvio: la seguridad se eleva y el tráfico en la red se reduce al mínimo.

Las zonas son un segmento de una retícula SAN y se emplean para conectar grupos de servidores con dispositivos de almacenamiento para el procesamiento de rutina, pero es posible cambiarlas como sean necesarias. Por ejemplo, es posible reconfigurar las zonas para permitir respaldos ocasionales a los dispositivos de almacenamiento que residen fuera de las zonas individuales. Sólo los miembros de una zona tienen acceso a la misma.

NOTA Los conjuntos de zonas son grupos que interoperan en la retícula. Cada conjunto de zona puede aceptar hasta 256 zonas. Todos los dispositivos en una zona ven sólo a los dispositivos asignados a la misma, pero cualquier dispositivo de esa zona puede ser miembro de otras zonas en el conjunto.

Aunque podría sonar que las VSAN y las SAN están cortadas con la misma retícula, por decirlo así, existe una importante distinción entre ambos.

Cuando se usa la zonificación, la segmentación no queda completa, porque ocurre dentro de la misma base de datos en el conmutador que hace cumplir las zonas y proporcionan servicios de dirección y enrutamiento. Por ejemplo, un mal funcionamiento de un nodo en la zona puede corromper la base de datos y hacer que toda la SAN se venga abajo.

Por otro lado, las VSAN pueden segmentar la base de datos. Así, cada zona definida es su propia red de almacenamiento única con su propia base de datos dedicada. Eso significa que si una VSAN tiene problemas, eso no afecta a las otras VSAN en el mismo conmutador.

NOTA Como recordatorio, un LUN es un identificador que se usa en un bus SCSI para distinguir entre dispositivos (unidades lógicas) con la misma identificación SCSI.

En una SAN, los dispositivos de almacenamiento se zonifican de manera típica en el nivel de dispositivo o nivel LUN:

- ▼ **Nivel de dispositivo** Cada usuario se restringe al uso de dispositivos específicos, como arreglos RAID o discos específicos.
- ▲ **Nivel LUN** Esto permite que el administrador asigne recursos en unidades lógicas, en vez de hacerlo en unidades físicas. Es decir, una zona LUN puede dispersarse a lo largo de varios dispositivos físicos. Como lo ilustra la figura 10-7, es fácil que los dispositivos alberguen varias zonas.

Aunque la zonificación es una gran herramienta para la administración de recursos, el establecimiento de las zonas no debe tomarse a la ligera. Al igual que la construcción de una casa, uno no se detiene en la ferretería, toma unas tablas, una caja de clavos, algunos bastidores y comienza a martillar. Es preciso planear las zonas con todo cuidado, para asegurar que se toma en cuenta el mejor uso del almacenamiento de SAN y del ancho de banda. Además, una vez que se han instalado las zonas, es más difícil mover el espacio de almacenamiento de un grupo de usuarios (por ejemplo, en la zona A) a otro grupo (en la zona B). Si esto se realiza, con frecuencia será necesario reinicializar, lo que provocará una interrupción

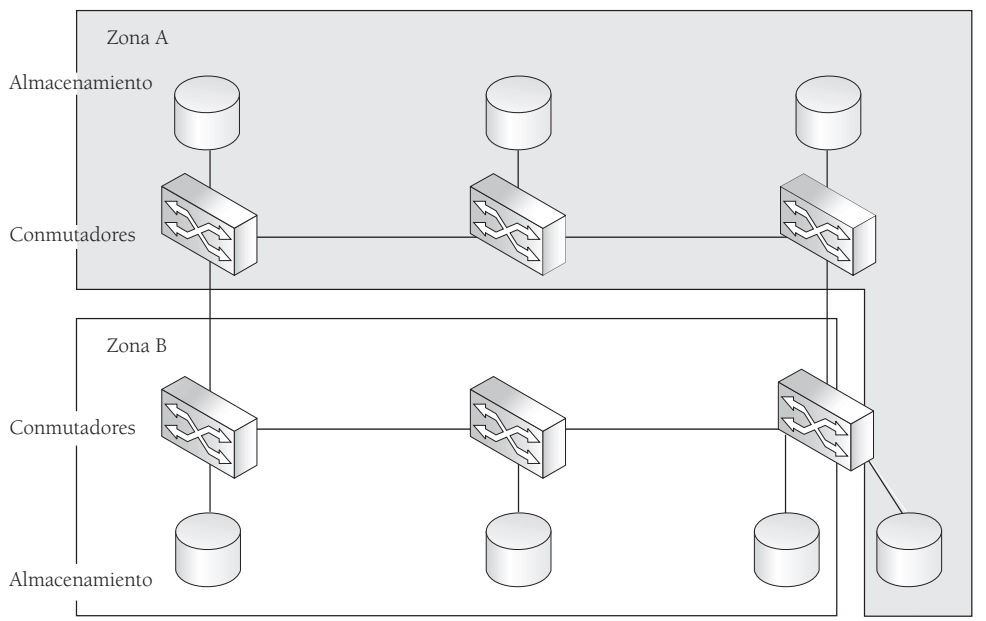


Figura 10-7. Es posible configurar las zonas para tener acceso a los recursos en diferentes dispositivos.

en la red. Aún peor, habrá vacíos de seguridad, ya que los usuarios en ambas zonas podrían terminar con el acceso al espacio de almacenamiento que se movió.

QoS

Quality of Service (QoS, calidad de servicio) es un atributo importante de la línea de conmutadores de MDS. En las versiones anteriores de Cisco SAN-OS (hablaremos con más detalle de este sistema operativo en páginas posteriores de este capítulo), el tráfico sólo se segmentaba si era de datos de control o datos de tráfico. En la versión más reciente de este sistema operativo, QoS permite clasificar el tráfico. Por ejemplo, es posible aplicar QoS de manera que los datos para el tráfico sensible a la latencia tengan mayor prioridad sobre las aplicaciones sensibles a los resultados, como el almacenamiento de datos.

Los conmutadores MDS proporcionan los siguientes mecanismos QoS:

- ▼ **Cola de prioridades** Se asignan niveles de prioridad a distintos tipos de tráfico. El tráfico sensible a la latencia tiene mayor prioridad que los otros tipos.
- ▲ **Fibre Channel Congestion Control (FCC, control de congestión de Fibre Channel)** Se trata de un mecanismo de control de flujo que se utiliza para aligerar la congestión en las redes FC. En esencia, cualquier conmutador en la red puede identificar la congestión, muestrear marcos de la cola congestionada y luego subir mensajes acerca del problema a la fuente. El conmutador más cercano a la fuente de la congestión puede reenviar las marcos a otros conmutadores o limitar el flujo de éstos desde el puerto que provoca el problema.

Seguridad

Al igual que en cualquier dispositivo o tecnología de redes en Internet, la seguridad es un aspecto importante. Quizá sea especialmente importante en las SAN, donde gran parte de los datos de la organización se mueven y almacenan. Lo último que se necesita es que un intruso entre a los archivos de su empresa y provoque trastornos.

Los conmutadores MDS tienen varias características de seguridad, cuyo objetivo es mantener sus datos seguros. Observemos más de cerca la línea de conmutadores MDS de mecanismos de seguridad.

Autentificación Los conmutadores MDS proporcionan el primer nivel de seguridad a través de sus métodos de autentificación. Ésta viene en dos formas:

- ▼ **Autentificación del usuario** Authentication, authorization and Accounting (AAA, autenticación, autorización y contabilidad), de las que hablamos en el capítulo 6, se emplea para validar a los usuarios, otorgar acceso y vigilar las actividades. Una vez que se enviaron el nombre de usuario y la contraseña, los conmutadores realizan la autenticación local, comparando las credenciales del usuario contra una base de datos local, o de forma remota, utilizando un servidor RADIUS.
- ▲ **Conmutador a conmutador y host a conmutador** La SAN-OS de Cisco utiliza el Fibre Channel Security Protocol (FC-SP, protocolo de seguridad Fibre Channel) para la autentificación de conmutador a conmutador y de host a conmutador. Esto se utiliza para desalentar cualquier interrupción que pudiera ocurrir si un dispositivo no autorizado intentara conectarse a la retícula.

Seguridad de puerto La seguridad del puerto asegura que sólo un equipo autorizado pueda conectarse a un puerto del conmutador determinado. Los dispositivos pueden ser un host, un objetivo o un conmutador y se identifican por su World Wide Number (WWN, número mundial). Esta característica garantiza que la SAN no se vea transgredida por un dispositivo no autorizado que intente conectarse a un puerto del conmutador.

Control de acceso VSAN Es posible asignar funciones, con base en las limitaciones de una VSAN específica. Por ejemplo, la función de administrador de la red, puede ser administrada para las tareas de establecimiento y administración de la configuración. Por otro lado, es posible otorgar a los administradores VSAN permiso para configurar y administrar sólo VSAN específicas. Se trata de una herramienta muy útil ya que limita los trastornos a la SAN. Más que un error de configuración que afecte a toda la SAN, se ubicaría en la VSAN en la que se hizo el cambio.

Acceso basado en funciones Ir de la mano con la autentificación de usuarios es un acceso con base en funciones. Este mecanismo limita el acceso al conmutador con base en el nivel específico de permisos que se haya otorgado a ese usuario. Es posible otorgar al usuario pleno acceso al equipo, o bien se pueden manejar niveles específicos de lectura y escritura de cada comando.

SPAN

Una característica única de la línea MDS 9000 de Cisco es el Switched Port ANalizer (SPAN, analizador de puerto conmutado). Éste vigila el tráfico en la red utilizando una interfaz Fibre Channel. El tráfico a través de esta interfaz Fibre Channel puede replicarse a un puerto conocido como *puerto de destino SPAN* (*puerto SD*). Es posible configurar cualquiera de los puertos Fibre Channel del conmutador como puertos SD. Cuando una interfaz se encuentra en la modalidad de puerto SD, no puede utilizarse con el tráfico normal de datos. Puede anexarse un analizador de Fibre Channel al puerto, para vigilar el tráfico SPAN.

Como lo sugiere el nombre, Remote SPAN (RSPAN, SPAN remoto) le permite vigilar el tráfico para las fuentes SPAN en conmutadores por toda la retícula Fibre Channel. El puerto SD de un conmutador remoto se emplea para propósitos de vigilancia. Normalmente, el conmutador remoto es diferente del conmutador de origen, pero se une a la misma retícula. La familia MDS 9000 de conmutadores permite la vigilancia remota del tráfico desde cualquier conmutador en la retícula, como si fuera el conmutador de origen.

SPAN no es invasor, porque los puertos Sidebar no reciben marcos; sólo transmiten copias del tráfico fuente SPAN y no afectan la redirección del tráfico de red. Además, es posible especificar VSAN como una fuente SPAN. Todas las interfaces en la VSAN seleccionada se incluyen como fuentes SPAN. El tráfico SPAN puede vigilarse en dos sentidos:

- ▼ **Ingreso** Se refiere al tráfico que entra al conmutador a través de una interfaz de origen. Este tráfico se copia al puerto SD.
- ▲ **Egreso** Se refiere al tráfico que sale de la retícula del conmutador a través de una interfaz de origen. Al igual que el tráfico de ingreso, éste también se copia al puerto SD.

Cuando la VSAN se selecciona como fuente, entonces todos los puertos físicos, además de los PortChannels (canales de puerto), se emplean como fuentes SPAN. Los puertos TE

se incluyen cuando el puerto VSAN del punto TE es el mismo que la VSAN de origen. Los puertos TE se ignorados si la lista configurada de VSAN admitidas tiene la VSAN de origen pero el puerto VSAN es diferente.

Truncamiento

Un recordatorio de nuestro análisis de las VLAN es el término *truncamiento.* El truncamiento existe dentro del mundo de SAN en forma muy similar a como lo hace en la de VLAN. El truncamiento se refiere a un InterSwitch Link (ISL, vínculo entre conmutadores) que lleva más de una VSAN. Los puertos de truncamiento envían y reciben marcos Extended ISL (EISL, ISL extendidas), como se muestra en la figura 10-8. Estos marcos contienen un encabezado EISL, que transporta la información de la VSAN. Una vez que se habilita EISL en un puerto E, ese puerto se convierte en un puerto TE.

NOTA ISL es un protocolo propiedad de Cisco que mantiene la información de la VSAN como flujos de tráfico entre el origen y el destino.

PortChannel

Es posible agregar los varios puertos de Fibre Channel a un solo puerto lógico, lo que brinda un aumento de ancho de banda, equilibrio de cargas y redundancia de vínculos. A esto se le conoce como *PortChannel* y permite agregar hasta 16 puertos físicos en un solo puerto lógico.

PortChannel es una tecnología útil, porque eleva el ancho de banda agregado en un ISL o EISL al distribuir el tráfico entre todos los vínculos del canal. Además, el tráfico está equilibrado en cuanto a cargas a través de varios vínculos. Este tráfico se identifica por Source ID (SID, identificador origen), Destination ID (DID, identificador de destino) u Originator exchange ID (OX ID, identificador de intercambio del originador).

PortChannel también proporciona redundancia para sus vínculos. Si uno falla, el tráfico se traslada a los vínculos restantes. Además, el protocolo superior no percibe al vínculo

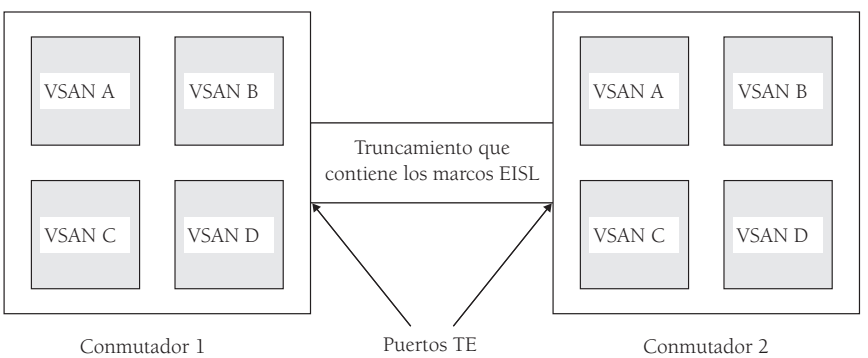


Figura 10-8. El truncamiento en una SAN combina varias conversaciones VSAN.

como falla. En cambio, simplemente tiene menos ancho de banda para trabajar. Así, las tablas de enrutamiento no se ven afectadas por una falla en los vínculos.

Hardware

La familia Cisco de productos MDS incluye dos Cisco MDS 9500 Series Multilayer Directors, el Cisco MDS 9216i Multilayer Fabric Switch y la Serie Cisco MDS 9100 de conmutadores de configuración fija, además de varios módulos, que proporcionan funcionalidad personalizada. Estos dispositivos proporcionan servicios inteligentes de red para SAN, incluidos VSAN, seguridad, administración del tráfico, diagnóstico y un entorno centralizado de administración.

Observemos más de cerca a los equipos en la línea Cisco MDS de conmutadores de almacenamiento multicapa.

Conmutadores MDS 9500 Multilayer Director

Los conmutadores MDS 9500 Multilayer Director son dispositivos modulares dirigidos hacia los entornos de grandes centros de datos. Proporcionan un alto nivel de escalabilidad, seguridad y administración.

La serie MDS 9500 incluye tres conmutadores multicapa:

- ▼ **Cisco MDS 9506 Director** Está dirigida hacia los entornos de centros de datos y posee 192 puertos de 4 Gbps y seis ranuras en el chasis, dos de las cuales se reservan para los módulos de supervisión. Es posible instalar cuatro módulos de conmutación o de servicios, lo que proporciona servicios de Fibre Channel o de Gigabit Ethernet. El plano posterior puede conectarse de manera directa a cuatro módulos de conmutación, dos módulos de supervisión, dos módulos de reloj y dos fuentes de poder.
- ■ **Cisco MDS 9509 Director** Orientado hacia grandes entornos de centros de datos, el chasis contiene 336 puertos Fibre Channel y nueve ranuras, dos de las cuales se reservan para los módulos de supervisión. Es posible instalar siete módulos de conmutación o de servicios, lo que proporciona servicios de Fibre Channel o de Gigabit Ethernet. El plano posterior puede conectarse de manera directa a siete módulos de conmutación, dos módulos de supervisión, dos módulos de reloj y dos fuentes de poder.
- ▲ **Cisco MDS 9513 Multilayer Director** Cisco introdujo este conmutador en agosto de 2002, pero luego lo retiró del mercado (al parecer, el mundo no estaba listo para este excelente conmutador). Lo reintrodujo en la primavera de 2006. El Cisco MDS 9513 Multilayer Director es un dispositivo Fibre Channel de 528 puertos orientado a las empresas que quieren consolidar sus SAN y suscribir los puertos en los conmutadores más pequeños. El conmutador presenta 13 ranuras y 528 puertos Fibre Channel de 4 Gbps. También soporta los protocolos iSCSI y FCIP.

Los módulos de supervisor de estos directores proporcionan alta disponibilidad y características de equilibrio de cargas. Un segundo módulo de supervisión está disponible con propósitos de redundancia. Además, los puertos Fibre Channel de autosensores soportan conexiones ISL (puertos E), EISL (puertos TE), ciclo (puertos FL y TL) y retícula (puertos F).

Los Small Form-factor Ports (SFP, puertos de forma-factor pequeños) de los directores son intercambiables y pueden configurarse para conexiones de longitud de onda corta (500 metros) o larga (10 kilómetros). Además, los puertos son configurables de manera individual para FCIP e iSCSI.

En la tabla 10-2 se comparan las características de MDS 9506, MDS 9509 y MDS 9513 de Cisco.

Conmutadores de retícula MDS 9000

Los "hermanos pequeños" de la serie MDS 9500 son los conmutadores Cisco MDS 9000. Emplean una arquitectura y una estructura de software similares a los directores de la serie 9500. Sin embargo, aunque la serie 9500 tiene un diseño plenamente modular, la serie 9000 es semimodular. Dentro de esta familia se encuentran dos series: el conmutador de retícula Cisco MDS 9216i y la serie Cisco MDS 9100.

Conmutadores de retícula multicapa Cisco MDS 9216 El Cisco MDS Multilayer Fabric Switch incluye tres modelos: Cisco MDS 9216, Cisco MDS 9216A y Cisco MDS 9216i. Estos conmutadores utilizan tanto Fibre Channel como IP en un solo módulo para una fuerte entrega del servicio. Los conmutadores soportan hasta 16 interfaces Fibre Channel de 2 Gbps y dos puertos Gigabit Ethernet para servicio FCIP e iSCSI.

El enrutamiento integrado VSAN e inter-VSAN permite una topología SAN de gran escala y sitios múltiples.

La capacidad de utilizar FCIP con los conmutadores MDS 9216 proporciona varios beneficios, entre los que se incluyen:

- Simplificación de la protección de datos y desempeño de la misión al permitir el respaldo, replicación remota y otros servicios de recuperación en una WAN.

	Cisco MDS 9506	Cisco MDS 9509	Cisco MDS 9513
Ranuras disponibles	6	9	13
Puertos por chasis Fibre Channel de 4 Gbps	192	336	528
Puertos por chasis Fibre Channel de 10 Gbps	16	28	44
Puertos por chasis iSCSI y FCIP	24	48	60
Unidades de gaveta	7	14	14
Chasis por gaveta	6	3	3
Puertos Fibre Channel por gaveta	1152	1008	1584

Tabla 10-2. Comparación de la serie Cisco MDS 9500.

- ▲ Son posibles las capacidades de la familia Cisco MDS 9000, incluidos VSAN, administración avanzada del tráfico y seguridad de red a través de conexiones remotas.

Los beneficios de los servicios iSCSI incluyen:

- ▼ La capacidad para conectarse a servidores anexos a Ethernet es mucho menos costosa que sólo poder conectarse a través de Fibre Channel.
- ▲ El almacenamiento aumenta y queda con mayor disponibilidad a través de la consolidación del almacenamiento de bloque de IP y Fibre Channel.

Los conmutadores MDS 9216 son modulares y soportan la línea de conmutación de la familia MDS 9000 o los módulos de servicios que se describen más adelante en este capítulo.

Conmutadores de Retícula Cisco MDS 9020 Dirigido hacia los negocios de tamaño pequeño o mediano que quieren construir su propia SAN, el conmutador de retícula Cisco MDS 9020 es un dispositivo Fibre Channel de 20 puertos que ofrece velocidades de hasta 4 Gbps. La administración se realiza a través del Administrador de Retícula MDS 9000 de Cisco y el Administrador de Dispositivos GUI, y la command-line interface (CLI, interfaz de línea de comando), similar al IOS.

Pequeño en su diseño, el conmutador de retícula Cisco MDS 9020 puede utilizarse como núcleo de una SAN pequeña o como dispositivo de vanguardia en una SAN mayor.

Serie Cisco MDS 9100 Las SAN de tamaño pequeño a mediano son atendidos con la serie 9100 Cisco MDS de conmutadores Fibre Channel. Los conmutadores (modelos 9120 y 9140) soportan 20 y 40 puertos, respectivamente, y son fijos en términos de expansibilidad. Como sus hermanos de alto rendimiento, la serie 9100 provee niveles altos de escalabilidad, disponibilidad, seguridad y administración.

La serie MSD 9100 incluye herramientas de administración SAN integradas (útil para la administración de uno de muchos dispositivos de retícula), incluida una herramienta de línea de comando y GUI, de la que hablaremos más adelante en este capítulo.

La arquitectura común y la estructura de software son una consideración importante cuando se analizan los dispositivos Cisco MDS. Debido a que poseen un diseño común, es fácil migrar de un dispositivo más pequeño a otro mayor, o bien agregar nuevos conmutadores a la retícula. Además, al igual que cualquier conmutador, el dispositivo puede ser adquirido e instalado con base en una necesidad específica dentro de la organización.

Por ejemplo, una organización de tamaño pequeño a mediano puede utilizar el Cisco MDS 9120 para construir su primera SAN cuando se desplaza de una solución de anexo directo a otra de almacenamiento en red. Las organizaciones de mayor tamaño podrían utilizar el 9120 para aplicaciones específicas o funciones de negocios.

Módulos

Al igual que muchos productos Cisco, es posible personalizar y configurar la familia MDS 9000 (excepto la 9100) con base en las necesidades particulares de su organización. Así, existen varios módulos que pueden instalarse en los equipos. Las siguientes secciones explican estos diversos módulos y la forma de utilizarlos mejor en su despliegue SAN.

Módulo de supervisión de la serie Cisco MDS 9500 Este módulo proporciona actualizaciones de software sin interrupciones y redundancia de hardware para una disponibilidad óptima. Puede reiniciar un proceso que haya fallado antes que la falla se detecte en el sistema. Esto es ideal, porque reduce el número de reajustes al módulo. Sin embargo, en los casos en los que se requiere un reajuste, el módulo de soporte de la unidad habrá tomado el control para eliminar las interrupciones a la SAN.

Con dos módulos supervisores instalados, un director de la serie 9500 puede proporcionar un ancho de banda de conmutación de 1.44 Tbps. También aporta puertos autosensores Fibre Channel de 1, 2 o 4 Gbps y es compatible con los futuros módulos de 10 Gbps.

Módulos de conmutación Fibre Channel Cisco MDS 9000 Se trata de módulos de 16 y 32 puertos. Cada uno de ellos es un protocolo múltiple de tres rangos Fibre Channel de intercambio, así como un módulo de Coarse Wavelength Division Multiplexing (CWDM, multiplexaje de división amplia de longitud de onda). Es posible configurar los puertos individuales con SFP de longitud de onda corta o larga, proporcionando conectividad de 500 metros y 10 kilómetros, respectivamente.

El CWDM SFP proporciona incluso mayores distancias entre equipos, de hasta 100 kilómetros. Las interfaces del módulo operan a 1, 2 y 4 Gbps. Los puertos pueden configurarse para operar como:

- ▼ Puertos E.
- ■ Puertos F.
- ■ Puertos FL.
- ■ Puertos FX.
- ■ Puertos Span Destination (SD, destino Span).
- ■ Puertos ST.
- ■ Puertos TE.
- ▲ Puertos TL.

Módulos de servicios de almacenamiento IP de la familia Cisco MDS 9000 Es posible agregar servicios IP a la familia de conmutadores MDS 9000 a través del uso del módulo de servicios de almacenamiento IP de la familia Cisco MDS 9000. Este módulo permite enrutar el tráfico entre un puerto de almacenamiento IP y cualquier otro puerto en un conmutador de la familia MDS 9000. Además de los servicios disponibles a través de otros módulos de servicio de almacenamiento (incluidos VSAN, seguridad y administración del tráfico), los módulos de servicios de almacenamiento IP de la familia Cisco MDS 9000 utiliza IP para proporcionar conexiones eficaces en cuanto a costos a más servidores y ubicaciones. Este módulo brinda servicios de almacenamiento FCIP e iSCSI IP:

- ▼ **FCIP** Proporciona protección de los datos permitiendo la copia de seguridad, la replicación remota y la recuperación de desastres a través de conexiones WAN, utilizando los túneles FCIP. Los recursos WAN se emplean de manera óptima haciendo túneles de hasta tres ISL en un solo puerto Gigabit Ethernet. Además, la complejidad de SAN disminuye, porque no es necesaria una plataforma de conectividad remota.
- ▲ **iSCSI** Uno de los mejores atributos de las características iSCSI del módulo de servicios de almacenamiento IP es la capacidad para utilizar almacenamiento con

base en SAN Fibre Channel en servidores con base en IP. Esto es mucho menos caro que el solo uso de Fibre Channel. El almacenamiento y la utilización aumentan porque IP y Fibre Channel se consolidan para propósitos de almacenamiento. Además, iSCSI permite el uso de aplicaciones de almacenamiento legendarias.

Módulo de servicios de caché Cisco MDS 9000 Cisco se asoció con IBM para producir el módulo de servicios de caché Cisco MDS 9000. Este módulo se emplea para crear virtualmente un dispositivo de almacenamiento a partir de dispositivos separados en toda la red. Esto proporciona acceso a más información y se maneja de forma central.

Este módulo emplea dos nodos que se combinan con el software de almacenamiento TotalStorage SAN Volume Controller Storage Software para Cisco MDS 9000, permitiendo la virtualización y replicación con host en la red.

Para disponibilidad y confiabilidad óptimas, cada módulo incluye 8 GB de caché local, baterías primarias y de respaldo y discos duros para proteger los datos durante las fallas de energía.

Software

Existen dos formas de manejar los conmutadores MDS: desde la línea de comando o utilizando el Cisco MDS 9000 Fabric Manager, una GUI. La interfaz de línea de comando (CLI) es similar al CLI que se usa para administrar los demás conmutadores y enrutadores Cisco. Por otra parte, la GUI proporciona una representación gráfica de la SAN, de su estado y de los equipos en ella. Antes de hablar del CLI y de la GUI, es útil entender el sistema operativo detrás de la familia MDS: Cisco SAN-OS.

Cisco SAN-OS

Cisco SAN-OS es el sistema operativo para la línea Cisco MDS de dispositivos SAN. Proporciona características de trabajo en red de almacenamiento, incluidos actualizaciones sin interrumpir el trabajo, integración de varios protocolos, VSAN, administración de tráfico, diagnóstico y una administración SAN unificada.

La versión más reciente del sistema operativo, Cisco MDS 9000 SAN-OS 1.3, incluye una versión basada en servidor de Cisco Fabric Manager, una herramienta gráfica incrustada de administración. Esta inclusión proporciona tres mejoras importantes: administración centralizada de retículas múltiples; salud, descubrimiento y vigilancia continuos; y vigilancia del desempeño.

Además, la seguridad en SAN-OS aumenta debido a la autentificación de conmutador a conmutador y de servidor a conmutador utilizando Fibre Channel Security Protocol (FC-SP, protocolo de seguridad Fibre Channel). Esto protege contra invasores de dispositivos no autorizados. También emplea TACACS+ para autentificación, autorización y contabilidad de los conmutadores.

CLI

La primera forma de administrar un conmutador Cisco MDS 9000 es utilizando una conexión serial RJ-45 en el módulo supervisor. Esta conexión, al igual que todas las que se hacen en otros enrutadores y conmutadores Cisco, proporciona acceso a la CLI.

Si elije utilizar CLI o Fabric Manager dependerá en gran medida del gusto y las preferencias personales. Sin embargo, existen algunos casos en que será preferible uno de los dos. Por ejemplo, CLI puede ser empleado de manera óptima cuando:

- ▼ Se realizan rutinas de establecimiento inicial.
- ■ Se ejecutan comandos de depuración y demostración, para diagnóstico y detección de problemas.
- ▲ Se escriben y ejecutan secuencias de comandos de configuración.

Cuando el dispositivo MDS se conecta de manera local por primera vez, el sistema ingresa una rutina de establecimiento que ayuda a la configuración inicial del dispositivo. Este paso debe completarse antes de que pueda conectar al conmutador o administrarlo con Cisco Fabric Manager.

El dispositivo CLI proporciona ayuda de comando, conclusión de comando y la capacidad de tener acceso a los comandos que se ejecutaron anteriormente. Ingresar los comandos es similar al proceso que se utilizó cuando se ingresaron los comandos en otros conmutadores Cisco. Por ejemplo, el comando siguiente se utilizaría para enviar un mensaje a todos los usuarios en la red de que el sistema cerrará para tareas de mantenimiento:

```
switch# send Shutting down the system in 5 minutes. Please log off.
```

Para entrar al modo de configuración, simplemente ingrese lo siguiente en el conmutador MDS:

```
switch# conf t
switch (config) #
```

Una vez que se está en el modo de configuración, el dispositivo puede administrarse utilizando varios comandos. En la tabla 10-3 se muestra una breve lista de algunos de estos comandos y una explicación de lo que hacen.

Comando	Descripción
Fcc	Para configurar el control de congestión FC.
Fcdomain	Para entrar al modo de configuración fcdomain.
QoS	Establece la prioridad de los marcos de control FC.
radius-server	Para configurar los parámetros RADIUS.
Vsan	Para entrar al modo de configuración VSAN.
Zone	Para entrar en los comandos de configuración de zona.

Tabla 10-3. Varios comandos de configuración que se utilizan en la CLI.

Cisco Fabric Manager

Dependiendo de sus preferencias, tal vez desee administrar su retícula MDS utilizando una interfaz de usuario gráfico. En este caso, Cisco ha proporcionado el Cisco Fabric Manager. Se trata de una herramienta de administración de dispositivos y retículas de redes basados en Java y SNMP que muestra visiones en tiempo real de la retícula y de los dispositivos instalados. Cisco Fabric Manager es una alternativa a CLI para casi todas las operaciones de administración de conmutadores y se incluye en los conmutadores.

Cisco Fabric Manager recolecta información acerca de la topología de la retícula y luego envía solicitudes SNMP al agente SNMP que opera sobre el conmutador al que se conecta Fabric Manager. Una vez que el conmutador ha descubierto todos los dispositivos conectados, responde a ellos. Recolecta esta información utilizando los datos de la base de datos FSPF, así como de la base de datos del servidor del nombre.

Fabric Manager se utiliza para descubrir y ver la topología de la retícula y administrar zonas. También es útil para la administración de:

- ▼ Zonas y conjuntos de zonas.
- ■ VSAN.
- ■ Canales de puertos.
- ▲ Usuarios y roles.

La GUI emplea tres vistas para administrar la retícula de la red:

- ▼ **Device View (vista dispositivo)** Muestra la exhibición actual de la configuración de dispositivo y las condiciones de desempeño para un solo equipo.
- ■ **Fabric View (vista retícula)** Muestra el estado actual de la retícula de la red, incluyendo varios dispositivos.
- ▲ **Summary View (vista resumen)** Muestra un resumen de los conmutadores, hosts, subsistemas de almacenamiento y VSAN. Muestra un resumen de la actividad de diferentes puertos, así como los dispositivos vecinos IP y FC.

Cisco Fabric Manager comprende dos herramientas de administración de red que soportan la versión 3 de Simple Network Management Protocol. Estas herramientas incluyen:

- ▼ **Fabric Manager (administrador de retícula)** Muestra un mapa de toda la retícula de la red, incluyendo no sólo los dispositivos Cisco MDS 9000, sino también conmutadores, hosts y dispositivos de almacenamiento de otros proveedores.
- ▲ **Device Manager (administrador dispositivo)** Muestra las vistas de Device y Summary de la retícula.

Almacenamiento adjunto de red

NAS, que se analizó al principio de este capítulo, es una buena opción para las organizaciones que necesitan una solución más pequeña y que pueda operar de manera exclusiva sobre IP. Lo esencial de este capítulo ha sido SAN, pero las soluciones NAS ciertamente tienen su lugar.

Cisco introdujo sus Cisco FS 5500 Series Integrated NAS y Cisco FS 5700 Series Integrated NAS para proporcionar funcionalidad NAS. Estos sistemas soportan Common Internet File System (CIFS, sistema de archivos de Internet comunes), Network File System (NFS,

sistema de archivos de red) y File Transfer Protocol (FTP, Protocolo de transferencia de archivos), así como protocolos de nivel de bloqueo y acceso de almacenamiento, incluyendo iSCSI.

Estas series pueden utilizarse en una de dos modalidades de operación, que proporcionan ya sea alto desempeño o alta confiabilidad. Estas modalidades son:

- ▼ **Primary/standby (primaria/espera)** Diseñada para entornos en los que se requiere alta disponibilidad. En esta configuración, uno de los Data Movers de NAS opera como espera plena, mientras que el otro maneja el movimiento de solicitudes de usuario entre red y almacenamiento.
- ▲ **Primary/primary (primaria/primaria)** Diseñada para los entornos en que se requiere un alto desempeño. Ambos Data Movers pueden configurarse para administrar las solicitudes de información. Si uno de los Data Movers falla, el NAS reinicializará a los pocos segundos.

En la tabla 10-4 se comparan los Cisco FS 5500 Series Integrated NAS y Cisco FS 5700 Series Integrated NAS.

La SAN es una tecnología que apenas comienza, y se espera que muchas organizaciones la adopten en los próximos años. Si bien Cisco tiene una solución sólida en su línea MDS de conmutadores, se espera que la empresa expanda su oferta SAN en los próximos años. Hay pocas dudas de que existe una creciente necesidad de SAN y almacenamiento avanzado, y éste será un tiempo interesante para cualquier persona interesada en la arena de almacenamiento.

	Cisco FS 5500 Series	Cisco FS 5700 Series
Configuración de Data Mover	Soporta las configuraciones sencilla y dual de Data Mover. Las configuraciones sencillas de Data Mover pueden actualizarse sin interrumpir el trabajo a las configuraciones duales de Data Mover.	Sólo la configuración dual de Data Mover.
CPU de Data Mover	CPU dual 1.6 GHz Pentium IV.	CPU dual 3.0 GHz Pentium IV.
Memoria de Data Mover	4 GB de RAM de tasa doble (266 MHz).	4 GB de RAM de tasa doble (266 MHz).
Conectividad Data Mover Fibre Channel	Dos puertos de 2 Gbps para la conectividad conjunto/conmutador.	Un puerto de 2 Gbps para la conectividad de cinta.

Tabla 10-4. Comparación de Cisco FS 5500 Series Integrated NAS y Cisco FS 5700 Series Integrated NAS (*continúa*).

	Cisco FS 5500 Series	Cisco FS 5700 Series
Conectividad Ethernet	Cuatro puertos 10/100/1000. Un puerto de administración 10/100.	Seis puertos 10 / 100 / 1000 (cobre). Dos puertos 1000 BASE-X Gigabit Ethernet (ópticos). Un puerto 10/100 de administración. Un puerto 10/100/1000 de administración.
CPU del procesador de almacenamiento	CPU dual 1.6 GHz Pentium IV.	CPU dual 3.0 GHz Pentium IV.
Memoria del procesador de almacenamiento	RAM de tasa doble de 2 GB (266 MHz).	RAM de tasa doble de 4 GB (266 MHz).
Conectividad de Fibre Channel del procesador de almacenamiento	Dos puertos de 2 Gbps para conectividad a Data Movers. Dos puertos de 2 Gbps para conectividad a Disk Array Enclosures.	Dos puertos de 2 Gbps para conectividad a Data Movers. Dos puertos de 2 Gbps para conectividad a Disk Array Enclosures.
Conectividad Ethernet del procesador de almacenamiento.	Un puerto de administración 10/100BASE-T.	Un puerto de administración 10/100BASE-T.

Tabla 10-4. Comparación de Cisco FS 5500 Series Integrated NAS y Cisco FS 5700 Series Integrated NAS (*conclusión*).

CAPÍTULO 11

Redes de contenido y soluciones de video de Cisco

Debido a que Internet continúa siendo un lugar rico en multimedia, es evidente que un solo servidor de una organización no puede llevar toda la carga por sí solo. Por ejemplo, cuando cientos de usuarios de todo el país traten de acceder al contenido multimedia de un servidor ubicado en Kansas City, los resultados serán menos que óptimos.

Sin embargo, si el contenido de ese servidor se replicara y se colocara en Seattle, Nueva York, Chicago, Atlanta, Kansas City y Reno, los usuarios podrían tener un acceso más rápido al material con menos carga en la red. A este tipo de red se le conoce como *Content Delivery Network* (*CDN, red de entrega de contenido*) y está ganando popularidad entre las organizaciones que buscan gran disponibilidad en sus redes.

REDES DE ENTREGA DE CONTENIDO

No sólo se encuentra más accesible el contenido gracias al hecho de que varios servidores sirven de hosts, sino que con una CDN instalada, un proveedor puede publicar contenido desde servidores de origen hacia los bordes de la red. Esto libera recursos en el servidor, haciendo que el contenido se localice y envíe al usuario de forma más sencilla, rápida y eficiente.

En esta sección, hablaremos acerca de las CDN, cómo trabajan y cómo pueden configurarse para ayudar a su organización. Además, echaremos un vistazo más de cerca a la solución CDN de Cisco, que incluye varias piezas de hardware y algún software de administración especializado.

Introducción a las CDN

Una CDN es una red de contenido, distribuida geográficamente para permitir una recuperación rápida y confiable desde cualquier lugar en que se encuentre el usuario final. Para apresurar la recuperación de contenido y transmisión, CDN usa tecnologías como almacenamiento en caché para llevar el contenido cerca del borde de la red. El hecho de equilibrar la carga a escala global asegura que se enrute a los usuarios de manera transparente al "mejor" origen de contenido. "Mejor" está determinado por varios factores, incluida la ubicación del usuario y los recursos disponibles en la red. El contenido almacenado se mantiene actual y protegido contra modificaciones no autorizadas.

Cuando un usuario hace una solicitud, los enrutadores de contenido determinan el mejor sitio, y los conmutadores de contenido encuentran un nodo para la entrega dentro del sitio. Los servicios inteligentes de red permiten seguridad integrada, Quality of Service (QoS, calidad de servicio) y Virtual Private Networks (VPN, redes privadas virtuales).

El mercado de CDN está creciendo. Lo que ha avivado el crecimiento es la demanda de servicios de Internet, como Web y el uso de host de aplicaciones, el comercio electrónico, los medios de transmisión de flujo y las aplicaciones multimedia. Mientras el usuario demanda estas enormes cantidades de servicio, el reto para los proveedores de servicio está en escalar sus redes que se encuentran ya congestionadas para aprovechar estas oportunidades de margen más alto.

Las necesidades de CDN

La CDN permite que el contenido Web sea almacenado en el caché en varios lugares de Internet. Cuando un usuario pide el contenido, una CDN enruta el pedido a un caché que sea conveniente para el cliente. Específicamente, busca uno que esté en línea, que se encuentre cerca y que no sea costoso comunicarse con él.

¿Qué organizaciones obtendrán los mejores resultados de una CDN? Como con cualquier tecnología y su capacidad de uso, ésta es una pregunta difícil. Como hemos visto una y otra vez, lo único que limita la manera en que se usa la tecnología, es la imaginación. Sin embargo, quienes se beneficiarían más de una CDN son los usuarios que tienen una demanda de archivos abundante o de multimedia, que exija demasiado de una sola red.

Sin embargo, hay un gran mérito en usar los principios CDN para asegurar la confiabilidad en caso de catástrofe. Por ejemplo, si está almacenando contenido en cachés en tres diferentes estados, un desastre natural en su estado natal no significa el fin de su interconexión. En cambio, los usuarios aún podrían acceder a la información de uno de los dos cachés restantes.

El uso de CDN no significa que todos sus datos se esparcirán por Internet. Puede controlar dónde se encuentra su contenido en la CDN y quién tendrá acceso a él. El contenido específico es asignado a cachés particulares, y sólo esos están autorizados a almacenar ese material. Al controlar donde se almacena, aumenta la probabilidad de que el contenido que se solicitó esté presente en el caché. Eso es porque hay suficiente espacio en el caché para almacenar todo el contenido autorizado. Además, al controlar el contenido se producen mejores resultados en el rendimiento, porque puede asegurar que un caché en particular sólo tenga el contenido cuyo almacenamiento se autorizó.

La compañía asegura que las CDN de Cisco permiten a los proveedores de servicio distribuir el contenido cerca del usuario final y atender los problemas de disponibilidad de ancho de banda, distancia u obstáculos de latencia, escalabilidad del servidor de origen y congestión de tráfico durante los periodos de uso pico. El sistema también permite a los negocios apresurar el despliegue de aplicaciones.

Una CDN no es un reemplazo para las redes convencionales. En cambio, suele usarse específicamente para contenido especializado que requiera gran disponibilidad. Por otra parte, el contenido dinámico o localizado puede utilizar el servidor de sitio de la organización, evitando la CDN, mientras que el contenido estático y fácilmente distribuido puede ser recuperado por el servidor CDN más cercano. Por ejemplo, los anuncios en carteleras, los applets y las imágenes, que representen casi el 70% de una página Web, pueden descargarse fácilmente en una CDN.

¿Cómo funciona?

La necesidad de CDN resulta especialmente evidente cuando se presenta contenido multimedia. Debido a que consume grandes cantidades de ancho de banda, un solo servidor no podría atender solicitudes múltiples y concurrentes de contenido rico en multimedia.

En la figura 11-1 se muestra el diseño básico de una CDN.

Digamos que está navegando en Internet y quiere ver un video en línea en el sitio Web de la Red de Entrega de Contenido (www.reconte.com). Debido a que ese video en particular es muy popular, lo desplegaron en su CDN. Esto es lo que sucede cuando hace clic en el icono del video:

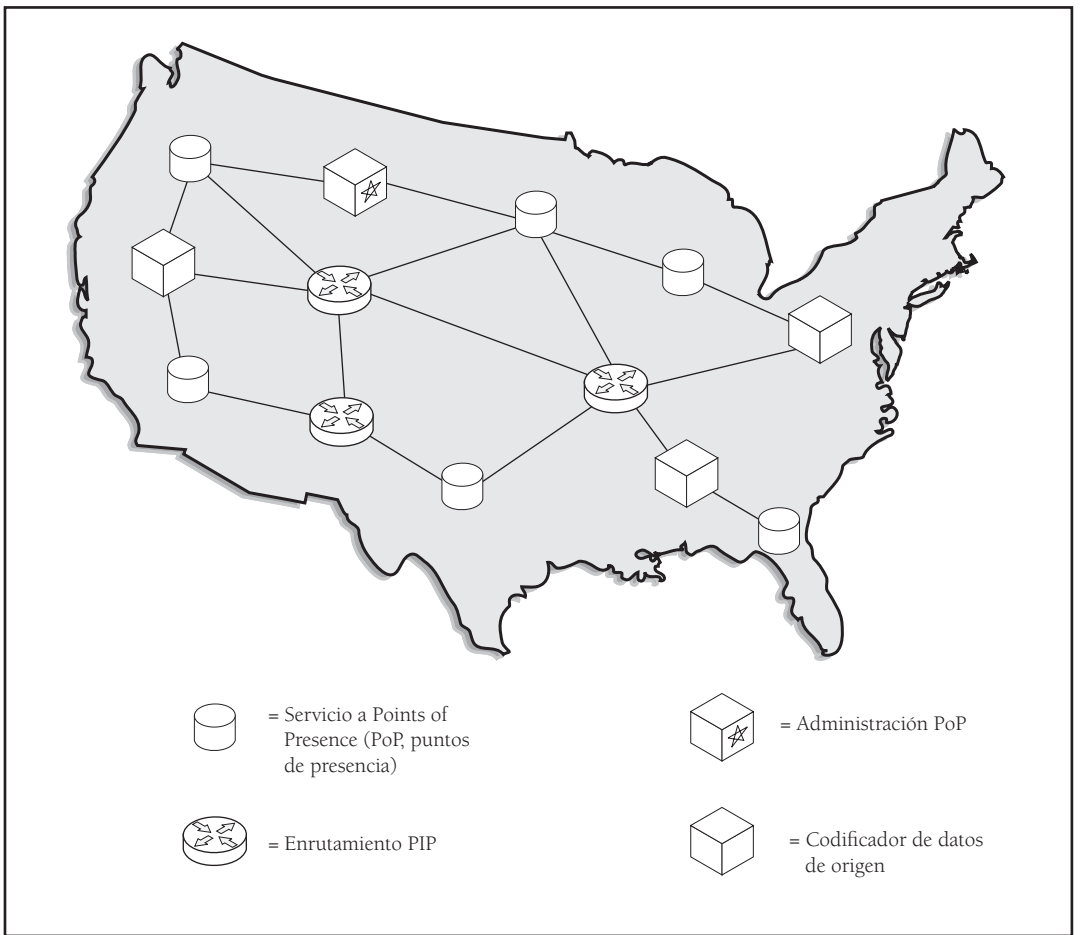


Figura 11-1. Un despliegue CDN básico incluye varios componentes.

1. El navegador del usuario solicita el URL de www.reconte.com/video.mpg.
2. La estación de trabajo del usuario realiza una búsqueda DNS de la dirección IP de www.reconte.com en un servidor proxy DNS local.
3. El servidor DNS local no tiene la dirección IP de www.reconte.com en el caché, así que consulta la jerarquía de DNS para determinar quién es el servidor DNS con autoridad. Después envía la solicitud a ese servidor DNS.
4. Si el entorno ha sido configurado correctamente, la consulta termina en el enrutador de contenido, porque su dirección IP es proporcionada de nuevo al servidor de proxy de DNS, el que, a su vez, envía esa dirección IP de regreso al solicitante original (la estación de trabajo del usuario).
5. El efecto neto es que el proceso ha dado como resultado una sustitución de la dirección IP real en el motor de contenido. Ahora el navegador puede pedir el archivo real asociado con el URL www.reconte.com/video.mpg.

6. Una vez que se recibe el archivo solicitado, el CE revisa si tiene la copia del archivo en el caché. Si la tiene, se envía al navegador solicitante. Si no se encuentra en el CE, éste traerá el archivo del sitio original (el sitio Web www.reconte.com), lo almacenará en el caché y enviará una copia al navegador.

En la siguiente solicitud del contenido asociado con www.reconte.com, la dirección IP debe estar ya almacenada en el caché para que la solicitud del cliente sea resuelta rápidamente a un buen CE. Si la dirección ya no se encuentra en el caché, los pasos se repetirán para encontrar el CE, y después proporcionará el contenido. Si se juzgó que el contenido ya no era actual, o ya no estaba ahí, se repetirá el proceso completo.

La solución de Cisco

CDN viene en una variedad de formas y configuraciones, basadas en gran parte en el vendedor y la necesidad. La solución CDN de Cisco está basada en cinco componentes (cada uno realiza una función específica en la máquina más grande). Esos componentes son:

- ▼ Administrador de distribución de contenido.
- ■ Motor de contenido.
- ■ Enrutamiento de contenido.
- ■ Entrega de borde de contenido.
- ▲ Interconectividad inteligente.

Sin importar qué datos se estén trasfiriendo (desde un archivo de texto hasta flujo de multimedia) el contenido se entrega usando estas tecnologías.

Administrador de distribución de contenido

El Content Distribution Manager (CDM, administrador de distribución de contenido) de Cisco se usa para distribuir automáticamente el contenido a los nodos de entrega de contenido localizados en el borde de la red. Esto permite la entrega global con monitoreo en tiempo real. Un CDM proporciona configuraciones de aprovisionamiento y directivas para todos los nodos de entrega de borde de contenido dentro de CDN. El Content Distribution Manager que se localiza en el punto central lógico de la red, permite la administración y el control de varios detalles como:

- ▼ Directivas del sistema.
- ■ Opciones de los dispositivos de red.
- ■ Control del contenido.
- ■ Réplica automática del contenido.
- ▲ Interfaz para el distribuidor de origen en vivo.

Físicamente, puede estar localizado dentro de un grupo local o distribuido geográficamente. Entre otras funciones del Content Distribution Manager se incluyen:

- ▼ Depósito central para monitoreo del sistema en tiempo real.
- ■ Administración del contenido, incluidos el registro en sitios Web y el flujo en vivo para permitir la entrega veloz y confiable.
- ■ Configuración redundante para tolerancia a fallos.
- ▲ Herramientas de publicación que permiten a los sitios Web suscribirse de manera sencilla al material de CDN sin mantenimiento y configuración caros.

La base de un sistema de distribución de contenido de Cisco es el Content Distribution Manager, que controla toda la red de distribución de medios.

Cisco solía producir aplicaciones CDM específicas; sin embargo, esos modelos han sido descontinuados y sus capacidades se pasaron a los motores de contenido.

Motores de contenido

Los motores de contenido de Cisco son productos de redes de contenido que aceleran la entrega de éste y se encuentran en el mismo lugar que el software Application and Content Networking System (ACNS, sistema de red de aplicación y contenido). Un motor de contenido es un dispositivo que almacena en el caché de un servidor CDN el contenido de las solicitudes de usuario final. Una colección de motores de contenido forma una CDN.

NOTA ACNS se explica más adelante en este capítulo.

En el pasado, Cisco produjo enrutadores de contenido individuales y CDM. Sin embargo, esta funcionalidad ahora se ha incorporado a su línea de motores de contenido.

NOTA Los motores de contenido pueden ser configurados como motores de contenido, enrutadores de contenido o administradores de entrega de contenido. Sin embargo, no pueden configurarse para realizar dos o más funciones. Es decir, un motor de contenido no puede configurarse como motor y enrutador de contenido. Tiene que configurarse como uno u otro.

El motor de contenido de Cisco funciona con su infraestructura de red existente para completar su solución de localización de tráfico. Los motores de contenido ofrecen un rango amplio de servicios de entrega de contenido para proveedores de servicios y empresas, incluidos medios de transmisión de flujo, servicio avanzado de almacenamiento en el caché transparente y administración de Internet por parte el empleado.

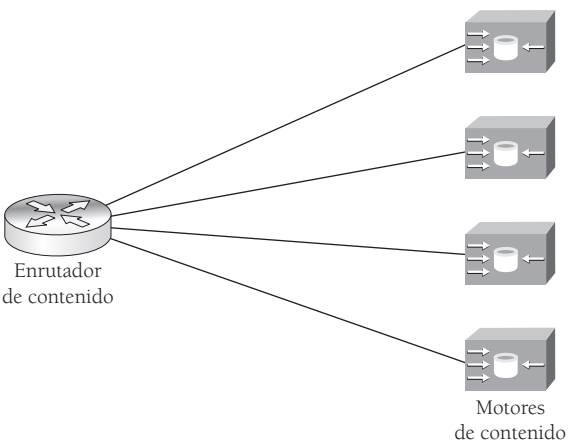
Los motores de contenido ofrecen un amplio rango de entornos, desde "Super Points of Presence (PoP, presencia de puntos) de proveedores de servicio hasta pequeños sitios de sucursales de empresas. La línea de productos de motores de contenido de Cisco incluye:

- **CE 7305** Este motor incluye una configuración de almacenamiento predeterminada de 144 GB, y es expandible hasta 936 GB. Se ejecuta en un procesador Intel Pentium 4 Prestonia a 2.4 GHz y cuenta con 2 GB de RAM. Este motor también puede conectarse a un puerto SCSI o al adaptador Fibre Channel del motor de contenido Cisco 7305 para servir como interfaz con SAN.
- **CE 7325** Este motor incluye una configuración de almacenamiento predeterminada de 432 GB y es expandible hasta 936 GB (aunque no se puede añadir más almacenamiento interno; tiene que expandirse externamente). Se ejecuta en dos procesadores Intel Pentium 4 Prestonia a 2.4 GHz y cuenta con 4 GB de RAM. Este motor también puede conectarse a un puerto SCSI o al adaptador Fibre Channel del motor de contenido Cisco 7325 para servir como interfaz con SAN.

- **CE 590** Esta aplicación de contenido es para proveedores de servicio de contenido PoP, sitios de colocación y sitios de empresas grandes. Es actualizable para soportar media de transmisión de flujo, viene equipado con dos discos duros de 36 GB. El almacenamiento es expandible hasta 252 GB. Tiene 16 MB de memoria flash y 1 GB SDRAM.
- **CE 565** El motor viene con 72 GB de almacenamiento en dos discos internos y puede expandirse hasta a 396 GB con el uso de hardware externo. El motor usa un procesador Intel Pentium 4 a 1.7 GHz y cuenta con 1 GB de RAM. El motor de contenido Cisco 565 puede configurarse con adaptadores Fibre Channel para servir como interfaz con SAN o con un decodificador de video MPEG para transmisión de video.
- ▲ **CE 507** Este motor viene con 18 GB de almacenamiento, con opción para 18 GB de almacenamiento adicional y 256 MB de RAM. Está diseñado como una plataforma de nivel de entrada para sucursales.

Enrutamiento de contenido

El enrutamiento de contenido es el mecanismo que dirige las solicitudes de los usuarios al sitio CDN. Esto permite una escalabilidad y confiabilidad altas. El enrutamiento se basa en un conjunto de variables en tiempo real, incluidos la demora, la topología, la carga de servidor y las directivas, como la ubicación del contenido y la autorización de un usuario. El enrutamiento del contenido permite la entrega acelerada del contenido y el enrutamiento adaptativo alrededor de conexiones rotas y congestionamientos en la red. Los productos de enrutador de contenido de Cisco interoperan con servicios inteligentes en una infraestructura de red, de tal modo que aseguran la disponibilidad del contenido y proporcionan un equilibrio de carga global.



Los nodos del enrutador de contenido son desplegados en ubicaciones estratégicas dentro de la red. Su funcionalidad incluye:

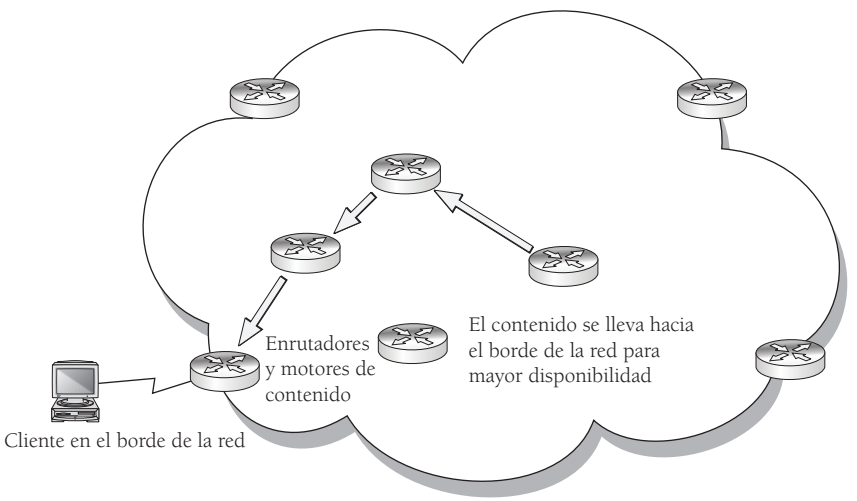
- Procesamiento de las solicitudes de contenido en tiempo real usando DNS estándar al redirigir las solicitudes del usuario a un motor de contenido apropiado basado en la ubicación geográfica, la ubicación de la red y las condiciones de ésta.
- Configuración redundante para tolerancia a fallos y equilibrio de carga de una red múltiple y de área amplia.

Cisco proporciona una gran cantidad de protocolos de enrutamiento de contenido que permiten a las empresas y a los proveedores de servicio construir redes de entrega de contenido. Estos protocolos permiten la comunicación sobre el estado del contenido entre los productos de conectividad de Cisco. Estos protocolos, entre los que se incluyen el Director Response Protocol (DRP, protocolo de respuesta directivo), Dynamic Feedback Protocol (DFP, protocolo de retroalimentación dinámico), Web Cache Control Protocol (WCCP, protocolo de control del caché Web) y Boomerang Control Protocol (BCP, protocolo de control bumerang), le permite a los productos de Cisco trabajar como un solo sistema.

Como los CDM, Cisco solía producir aplicaciones de contenido específico. Sin embargo, esos modelos también se han descontinuado y sus capacidades se traspasaron a los motores de contenido.

Entrega de contenido en el borde

Para acelerar este proceso, la entrega de contenido en el borde (realizada por los motores de contenido) distribuye el contenido del borde de la red al usuario final. La solución CDN de Cisco permite a los proveedores de servicio definir y expandir el borde de su red a cualquier lugar, desde un número pequeño de centros de datos cerca del núcleo de la red, hasta fuera del borde de la red y justo dentro del firewall de un consumidor.



Los motores de contenido están localizados en el borde de la red, almacenando y entregando contenido a los usuarios. Entre otras funciones se incluyen:

- ▼ Entrega de contenido a usuarios finales y otros motores de contenido basados en la tecnología de enrutamiento de contenido de Cisco.
- ■ Auto-organización en una jerarquía de enrutamiento de malla con otros motores de contenido formando la mejor topología lógica basada en la carga de la red actual, la proximidad y el ancho de banda disponible.
- ■ Almacenamiento de réplicas de contenido.
- ■ Servidores de punto final para todos los tipos de medios.
- ▲ Plataforma para medios de transmisión de flujo y aplicaciones de servicio.

Una vez que las bases correctas de la red están en su lugar, las cachés de la red se añaden en puntos estratégicos dentro de la red existente, con lo que se completa la solución de localización del tráfico. Las cachés de la red almacenan el contenido al que se ha tenido acceso con más frecuencia y después satisfacen las solicitudes localmente para el mismo contenido, eliminando transmisiones repetitivas de contenido idéntico sobre los vínculos WAN.

Conmutación del contenido

La conmutación del contenido se utiliza para equilibrar la carga de tráfico de forma inteligente a través de nodos de entrega a varios PoP o centros de datos distribuidos, con base en la disponibilidad del contenido, la disponibilidad de la aplicación y la carga del servidor. La conmutación inteligente de contenido añade una capa adicional de protección contra multitudes y asegura la continuidad de las transacciones para las aplicaciones de comercio electrónico frente a detenciones del sistema. La conmutación inteligente de contenido también permite la personalización de contenido para usuarios seleccionados y tipos de datos.

Cuando Cisco entró al juego de las CDN por primera vez, no desarrolló conmutadores que estuvieran destinados sólo para las CDN. En cambio, la funcionalidad CDN fue incluida como un componente de otros tipos de conmutadores de Cisco. Sin embargo, ahora, Cisco ha desarrollado sus Content Services Switches de la serie CSS 11500. Estos conmutadores tienen la funcionalidad de trabajar en cooperación con otros dispositivos en la solución CDN de Cisco.

Existen tres modelos en la línea Content Services Switches de la serie CSS 11500 de Cisco:

- ▼ **CSS 11501** Este modelo tiene una configuración fija, ofrece 6 Gbps de velocidad de transmisión de datos agregada, ocho puertos 10/100 Ethernet y un puerto Gigabit Ethernet, a través de un convertidor de interfaz. Este modelo soporta dos discos de memoria flash de 256 MB, dos discos duros de 512 MB y puede conducir hasta 1 000 transacciones SSL por segundo.
- ■ **CSS 11503** Este modelo tiene tres ranuras, ofrece 20 Gbps de rendimiento de procesamiento agregado, 32 puertos 10/100 Ethernet y seis puertos Gigabit Ethernet a través de convertidores de interfaz. Este modelo soporta hasta dos discos de memoria flash de 256 MB y hasta dos discos duros de 512 MB.
- ▲ **CSS 11506** Este modelo tiene seis ranuras, ofrece 40 Gbps de rendimiento de procesamiento agregado, 80 puertos 10/100 Ethernet y ocho puertos Gigabit Ethernet a través de los convertidores de interfaz. Requiere un módulo de conmutador de control. Este modelo soporta hasta dos discos de memoria flash de 256 MB y hasta dos discos duros de 512 MB.

Servicios inteligentes de red

El corazón de las CDN late por los servicios de red inteligentes. Éstos proporcionan funciones como seguridad, QoS, VPN y transmisiones múltiples. Los sistemas CDN de Cisco se integran con los servicios conscientes del contenido, que son necesarios para construir una CDN inteligente.

Entre los servicios clave que proporcionan inteligencia de contenido se incluyen:

- ▼ Enrutamiento de contenido.
- ■ Asignación de prioridad al tráfico de contenido.
- ■ Servicios que se escalan económicamente y que responden apropiadamente a las impredecibles multitudes relámpago.
- ▲ La habilidad de rastrear las solicitudes de contenido y responder con actualizaciones de contenido y replica.

Debido a que la funcionalidad de una CDN es dependiente del procesamiento de diversas variables, los servicios de red inteligentes son cruciales para mantener una CDN eficiente y efectiva.

Transmisiones múltiples IP

Las transmisiones múltiples IP son una manera eficiente (en relación con el ancho de banda) de enviar los mismos datos de transmisión de flujo a varios clientes. Entre las aplicaciones que se benefician de las transmisiones múltiples IP se incluyen videoconferencias, comunicaciones corporativas y aprendizaje a distancia. En vez de consumir grandes cantidades de ancho de banda al enviar el mismo contenido a varios destinos, los paquetes de transmisión múltiple se replican en la red en el punto en el que las rutas se separan. Esto da como resultado una manera eficiente de conservar recursos de red.

Cómo funciona La transmisión múltiple IP es ideal cuando un grupo de hosts de destino están recibiendo la misma transmisión de flujo de datos. Este grupo podría estar formado por cualquiera, en cualquier lugar. Podría ser un video con instrucciones enviado a todos los nuevos empleados de las oficinas centrales de la compañía, o información actualizada de las prestaciones enviada, simultáneamente, a los departamentos de recursos humanos de varias sucursales. Los hosts podrían estar localizados en cualquier lugar en Internet o en una red privada.

Ahora examinaremos los diferentes tipos de servicios de transmisión para ahondar, de forma precisa, en el funcionamiento de una transmisión múltiple. Consideremos primero los diferentes tipos de tráfico de la red (una sola transmisión, transmisión y transmisión múltiple) como se muestran en la figura 11-2:

- ▼ **Una sola transmisión** Las aplicaciones envían una copia de cada paquete a los usuarios que solicitan la información. Si un usuario se está vinculando al servidor Web y solicita información, esto no es tan malo. Sin embargo, si varios usuarios quieren el mismo contenido, esto devora los recursos del sistema mientras los mismos paquetes se envían a cada usuario de forma simultánea. Es decir, si 30 usuarios solicitan el mismo contenido, se enviarán 30 copias de los datos al mismo tiempo.
- ■ **Transmisión** Las aplicaciones pueden enviar una copia de cada paquete a una dirección de transmisión. Es decir, la información se envía a todos en la red. Aun-

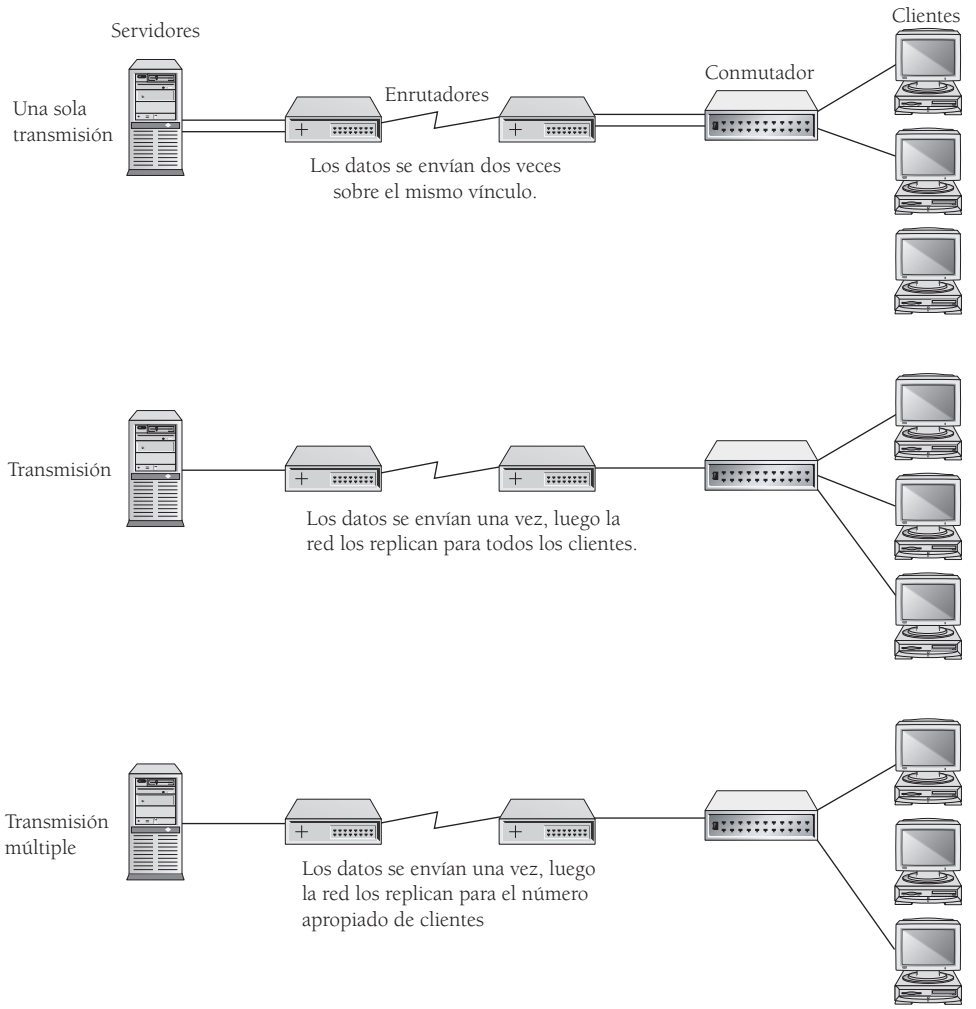


Figura 11-2. Los diferentes tipos de tráfico de red incluyen una sola transmisión, transmisión y transmisión múltiple.

que esto preserva ancho de banda, porque el mismo contenido se está enrutando a todos (en lugar de enviar a la vez varias copias del contenido), se complica porque habrá veces en que varios usuarios no desearán ni necesitarán ver el contenido.

- **Transmisión múltiple** Las aplicaciones envían una copia del paquete y la dirección a un grupo de receptores. La transmisión múltiple depende de que la red reenvíe los paquetes a las redes y hosts que las necesiten. De esta manera, se controla el tráfico de la red y se reduce la cantidad de procesamiento realizado por los hosts.

La transmisión múltiple tiene gran número de ventajas sobre las otras dos (una sola transmisión y transmisión). Aunque una sola transmisión es una manera efectiva de traer el contenido a un solo host, cuando el mismo contenido necesita ser enviado a varios hosts, puede inutilizar la red al consumir ancho de banda. Las transmisiones, por el otro lado, son una buena forma de conservar recursos de red (una sola copia de los datos se envía a cada usuario de la red). Aunque esto resuelve los problemas del consumo de ancho de banda, no es útil si sólo algunos usuarios necesitan ver la información.

La transmisión múltiple IP resuelve los problemas de cuello de botella cuando los datos se transfieren desde un emisor a varios destinos. Al enviar una sola copia de los datos a la red y permitiendo que ésta replique los paquetes a sus destinos, el ancho de banda se conserva para ambos, el emisor y el receptor.

En la figura 11-3 se muestra como la transmisión múltiple IP entrega los datos de una fuente a varios receptores apropiados. En este ejemplo, los usuarios quieren ver el video que los capacitará en una nueva aplicación. Los usuarios permiten que el servidor sepa que están interesados en ver el video al enviar un informe de host IGMP (Internet Group Management Protocol, protocolo de administración de grupo de Internet) a los enrutadores de la red. Éstos usan PIM (Protocol Independent Multicast, transmisión múltiple independiente del protocolo) para crear un *árbol de distribución de transmisión múltiple.* El flujo de datos se entregará sólo a los segmentos que se encuentren entre el origen y los receptores.

Los usuarios optan por ser parte de un grupo al enviar un mensaje IGMP. El IGMP es un protocolo de capa 3, lo que permite a los hosts indicarle a un enrutador que están interesados en recibir el tráfico de transmisión múltiple para un grupo o varios grupos en particular. En la versión 2 de IGMP se agregó la capacidad de dejar un grupo. Esto hizo más sencillo

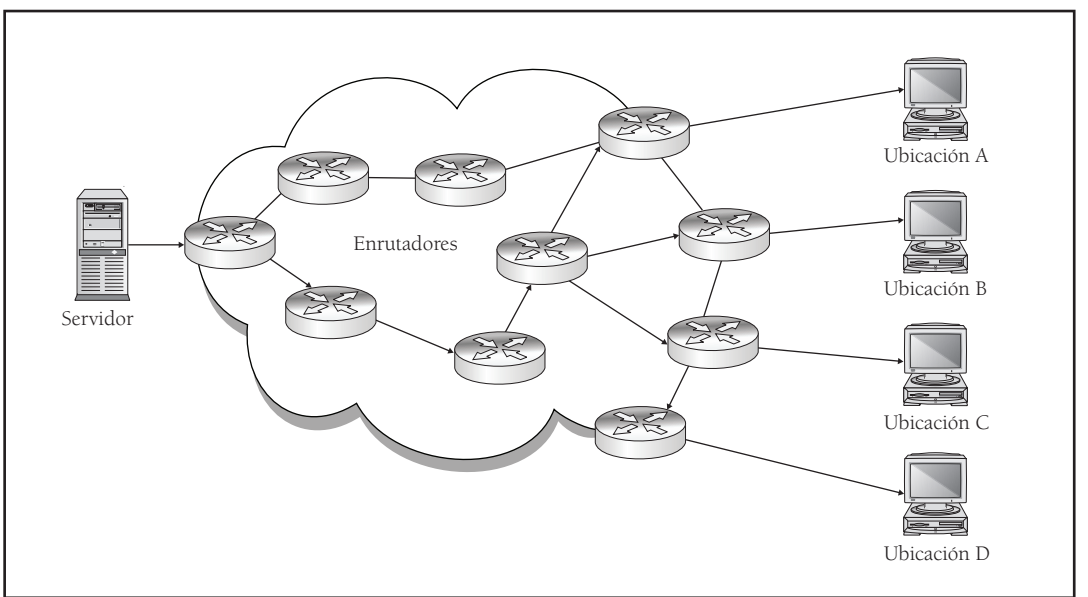


Figura 11-3. Los árboles de distribución de transmisión múltiple envían contenido a los segmentos de red apropiados.

para los enrutadores saber que cierto host ya no estaba interesado en recibir la transmisión múltiple, y así liberar más recursos de red.

Direccionamiento El direccionamiento es un componente importante en el mundo del la transmisión múltiple IP. Cuando un cliente opta por ser parte de un grupo, el contenido es entregado a una sola dirección IP. Cuando los datos se envían a esa dirección IP, la red, a su vez, entrega los datos a todos los que aceptaron estar en el grupo de transmisión múltiple. Al usar una sola dirección IP, la red puede manejar la tarea de canalizar los datos a los clientes apropiados.

La Internet Assigned Numbers Authority (IANA) administra la asignación de las direcciones de transmisión múltiple IP. Ha asignado el espacio de direcciones de clase D para uso en aplicaciones de transmisión múltiple IP. El espacio de direcciones de clase D está entre 224.0.0.0 y 239.255.255.255. No existen direcciones de host dentro del espacio de direcciones de clase D, porque todos los hosts del grupo comparten la misma dirección IP común de grupo.

Sin embargo, esto no quiere decir que una dirección de transmisión múltiple se vaya a ajustar a todas y cada una de las necesidades. Dentro del espacio de direcciones de clase D, las direcciones IP se han subdividido para uso especializado. A continuación se examina la manera en que el espacio de direcciones de clase D se estratifica aún más:

- ▼ **De 224.0.0.0 a 224.0.0.255** Para ser usadas sólo por protocolos de red en un segmento de red local. Un enrutador no puede reenviar los paquetes con estas direcciones. En cambio, éstas se quedan en el segmento LAN y siempre se transmiten con un valor TTL de 1.
- ■ **De 224.0.1.0 a 238.255.255.255** Llamadas de direcciones de *alcance global* y se usan para transmisión múltiple de datos entre la fuente y a través de Internet.
- ▲ **De 239.0.0.0 a 239.255.255.255** Llamadas de direcciones de *alcance limitado* o *alcance administrativo* y están atadas a una organización. Los enrutadores están configurados con filtros para prevenir al tráfico de las transmisiones múltiples en este rango, al salir de la red privada. Además, dentro de la organización, este rango de direcciones puede subdividirse dentro de límites internos, lo que permite volver a utilizar las direcciones en dominios más pequeños.

El *direccionamiento GLOP* es otro medio para el direccionamiento de la transmisión múltiple. RFC 2770 sugiere que el rango de direcciones 233.0.0.0/8 se reserve para direcciones en organizaciones que ya tengan reservado un Autonomous System Number (ASN, número de sistema autónomo). El ASN del dominio será después convertido y formará parte de un segundo o tercer octeto del rango 233.0.0.0/8 para generar una dirección de transmisión múltiple estática para esa organización.

NOTA Un ASN es un identificador único global para un sistema autónomo. Los sistemas autónomos son grupos de redes que tienen una sola política de enrutamiento administrada por los mismos operadores de red.

Por ejemplo, una organización con un ASN de 24545 tendría una dirección de transmisión múltiple IP de 233.95.225.0. Esta conversión primero toma el ASN (24545) y lo convierte en hexadecimal. El valor hexadecimal está separado en dos octetos y después se vuelve a convertir a decimal para darnos una subred que está reservada para uso con ASN 24545.

ACNS

Una CDN es un entorno que cambia de forma constante. Se añaden y se quitan motores de contenido, conmutadores de contenido y enrutadores de contenido, y el contenido almacenado en esos dispositivos está en un estado constante de flujo, porque los proveedores de contenido van y vienen. Se definen nuevos dominios enrutados, se quitan los anteriores se quitan y cambian las asignaciones de los dominios enrutados a motores de contenido.

El software Application and Content Networking System (ACNS, sistema de conectividad de aplicación y contenido) de Cisco está enfocado a las organizaciones y proveedores de servicio que despliegan varios CDN. Y la ACNS 5.3 es la versión más reciente de este software, que se ejecuta en los motores de contenido y en Wide Area Application Engine (WAE, motor de aplicación de área amplia), que combina componentes de red de contenido en una aplicación común para el Content Distribution Manager, motor de contenido y enrutador de contenido. Esta aplicación es útil para despliegues pequeños y grandes de CDN.

ACNS es una aplicación central detrás de las soluciones de video CDN e IP de Cisco. Permite que se transmita contenido y video desde el centro de datos a otras ubicaciones remotas, que incluyen:

- Contenido seguro Web.
- Aceleración de aplicación Web.
- Video de negocios.
- Video de punto de venta y quioscos Web.

NOTA ACNS también puede utilizarse para entregar actualizaciones de antivirus y parches de seguridad a través de una red.

ACNS puede manejar despliegues CDN de hasta 2 000 motores de contenido y 1 000 000 de artículos posicionados en motores de contenido. El software ACNS extrae el contenido de un servidor Web o FTP y lo envía directamente a los motores de contenido.

ACNS combina almacenamiento en caché extraído bajo demanda y posicionamiento previo para acelerar la entrega de aplicaciones Web, objetos, archivos y multimedia. ACNS se ejecuta en motores de contenido, CDM y enrutadores de contenido de Cisco.

En un entorno de video IP, ACNS puede utilizarse con los componentes IP/TV de Cisco, para capturar y entregar video MPEG con presentación sincronizada, creación de programa y programación.

En un entorno CDN, los motores de contenido pueden utilizarse con el Content Service Switch de la serie CSS 1150 de Cisco, el Content Switch Module de la serie Catalyst 6500 y los módulos conmutados de Secure Sockets Layer (SSL, capa de conectores seguros) para almacenamiento en caché de proxy inverso, lo que descarga a los servidores finales.

NOTA El almacenamiento en caché de proxy inverso, se explica más adelante en este capítulo.

ACNS se beneficia de un gran número de características, incluida la capacidad de configurar el sistema para ejecutar las aplicaciones de caché y CDN simultáneamente. Los administradores de red también pueden actualizar el software ACNS, o regresar a una versión instalada previamente, si determinan que la nueva versión no es tan útil como la instalación

previa. ACNS también permite el aprovisionamiento de disco, proporcionando la administración de espacio en disco para el almacenamiento en caché HTTP y para el contenido con posicionamiento previo.

Motor de aplicación de área amplia

La serie Wide Area Application Engine (WAE) de Cisco es una línea de aplicaciones de red que proporcionan acceso a aplicaciones, almacenamiento y contenido a través de WAN. WAE se usa junto con ACNS y el software Wide Area File System (WAFS, sistema de archivos de área amplia), del que hablaremos más en la siguiente sección. Estos productos y tecnologías permiten el acceso parecido a LAN a aplicaciones y datos a través de WAN. Entre algunos de los beneficios de esta solución se incluyen:

- ▼ Aplicaciones empresariales, como Enterprise Resource Planning (ERP, planeación de recursos empresariales), Customer Relationship Management (CRM, administración de relación con el consumidor) y portales de intranet.
- ■ Videoconferencias en tiempo real.
- ▲ Almacenamiento.

Más aún, WAE permite que las sucursales puedan utilizar infraestructura a través de WAN, incluidos servidores, copias de seguridad y almacenamiento, mientras coloca una sola aplicación WAE en cada sucursal. Esto se ilustra en la figura 11-4.

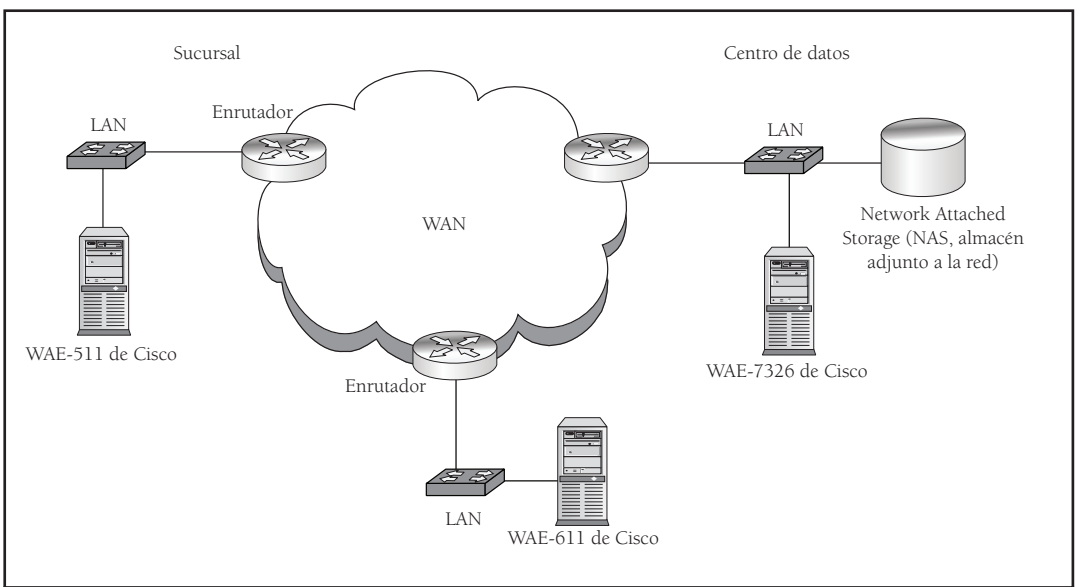


Figura 11-4. Los WAE reducen la carga de almacenamiento en las sucursales, reuniéndola en un centro de datos.

Los motores de aplicación WAE incluyen:

- ▼ **Cisco WAE-512 Wide Area Application Engine** Este dispositivo está basado en un procesador Intel Celeron a 3.0 GHz y está dirigido a pequeñas oficinas. La unidad viene con 1 GB de memoria y es expandible a 2 GB. Tiene dos bahías de disco duro Serial ATA para una capacidad de almacenamiento de entre 80 y 500 GB de capacidad. La unidad puede ser adaptada con un Fibre Channel o Host Bus Adapter (HBA, adaptador de bus host) para servir como interfaz con SAN o un codificador de video MPEG.
- ■ **Cisco WAE-612 Wide Area Application Engine** El siguiente escalón hacia arriba es el WAE-612 de Cisco. Al usar un 3 GHz Intel Pentium procesador 4, el WAE-612 tiene más memoria que los 512, con un máximo de 4 GB (viene con un estándar 2 GB de RAM). Esta unidad tiene dos bahías de disco duro Serial ATA y puede almacenar entre 292 y 600 GB de capacidad total. La aplicación puede adaptarse con Fibre Channel o HBA para hacer interfaz con SAN o un codificador de video MPEG.
- ▲ **Cisco WAE-7326 Wide Area Application Engine** La línea tope de WAE es el WAE-7326. Éste usa dos procesadores Intel Xeon y 4 GB de memoria. Soporta de dos a seis discos duros SCSI internos para una capacidad total de 1.8 TB. La unidad puede adaptarse con Fibre Channel o HBA para hacer interfaz con SAN o un codificador de video MPEG.

Sistema de archivos de área amplia

Otro componente de la solución CDN WAN de Cisco es el Wide Area File Services (WAFS, sistema de archivos de área amplia). Éste elimina la latencia WAN y las limitaciones de ancho de banda, y se esfuerza por dar velocidad y ancho de banda parecidas a LAN a los usuarios WAN. Esta tecnología ayuda a la consolidación de datos de sucursales dentro de servidores de archivos centrales en el centro de datos de la organización.

Beneficios

Al centralizar los datos de la organización, en vez de conservarlos dispersos por todas las sucursales, se pueden obtener los siguientes beneficios:

- ▼ **Costos más bajos** Los servicios de archivos e impresión en las sucursales remplazan las copias de seguridad en cinta y los servidores de archivos poco fiables y costosos.
- ■ **Protección mejorada de datos** Los datos generados en las sucursales son enviados al centro de datos en tiempo real. Esto mejora la protección de los datos, la administración y la eficiencia del almacenamiento.
- ■ **Administración reducida** Los datos pueden administrarse centralmente en el centro de datos.
- ▲ **Acceso e intercambio rápido de archivos** Con velocidades parecidas a LAN ahora en una WAN, los usuarios remotos pueden disfrutar de un aumento en la productividad.

WAFS utiliza nuevas tecnologías de optimización de protocolo para dar a las sucursales y usuarios de oficina remotos velocidades LAN, lo que reduce las limitaciones de latencia WAN, ancho de banda y paquetes perdidos.

Las sucursales consolidan sus servidores de archivos y su almacenamiento en servidores de archivos centrales o Network-Attached Storage (NAS, almacén adjunto a la red) en el centro de datos de la organización.

¿Cómo funciona?

WAFS usa optimizaciones de protocolos, incluidas:

- ▼ Mitigación de latencia.
- ■ Almacenamiento de un objeto en el caché.
- ■ Almacenamiento en caché de metadatos.
- ▲ Optimizaciones de transporte WAN.

Esto asegura la operación de los protocolos estándares de sistema de archivos, como Common Internet File System (CIFS, sistema común de archivos de Internet) con Windows y Network File System (NFS, sistema de archivos de red) con UNIX. Esto mantiene la integridad y las políticas de seguridad de los archivos.

WAFS 3.0 se ejecuta en el Wide Area Aplication Engines que se describió en la sección anterior. Además de las aplicaciones WAE, WAFS se ejecuta en el modulo de red con enrutador integrado.

Dentro de una solución WAFS, cada nodo puede ser configurado con uno o más servicios:

- ▼ **El motor de archivos de borde (Edge File Engine)** Usado en sucursales para remplazar a los servidores de archivos e impresoras, esto permite que los usuarios disfruten velocidades cercanas a LAN con acceso de escritura y lectura al centro de datos.
- ■ **El motor central de archivos (Core File Engine)** Usado en el centro de datos y conectado a través de LAN a dispositivos NAS, este motor es responsable de proporcionar servicios de agregación para motores de archivos de borde.
- ▲ **El administrador central WAFS de Cisco (Cisco WAFS Central Manager)** Proporciona administración basada en Web y monitoreo de todos los nodos WAFS.

NOTA Mediante WAE las aplicaciones pueden configurarse con cualquier servicio; sólo el módulo de red con enrutador integrado puede ser configurado como motor de archivos de borde.

En la figura 11-5 se muestra un ejemplo de cómo se despliegan estos servicios.

ALMACENAMIENTO EN EL CACHÉ

Por años, el tráfico de Internet ha ido creciendo a pasos agigantados. Debido a la enorme cantidad de tráfico que recorre Internet y las intranets, la congestión ha ido empeorando. Los ISP y organizaciones están siendo desafiadas para lidiar con ese problema, porque es difícil asegurar QoS y entregar el contenido a los clientes de forma eficiente y costeable. Al localizar los patrones de tráfico en su red existente, obtiene un doble beneficio: no sólo se entrega el contenido más rápido, sino que también los recursos liberados quedan disponibles para tráfico adicional.

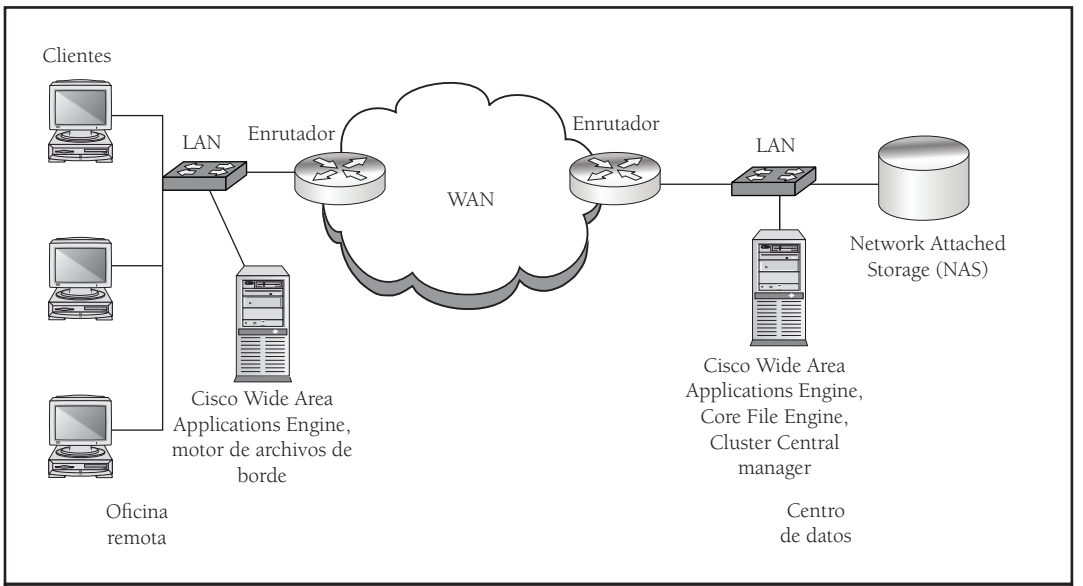


Figura 11-5. Las aplicaciones WAE se configuran para deberes de contenido específico dentro de la red.

La entrega del contenido se acelera al rellenar de forma local las solicitudes de contenido, en vez de tener que recorrer Internet para traer la información. Esto asegura que el contenido se entregue de forma rápida y no tendrá que preocuparse por los cuellos de botella más allá de su control. La ubicación del tráfico reduce la cantidad de tráfico redundante en sus conexiones WAN. Esto permite recursos adicionales de red para más usuarios y para nuevos servicios (como VoIP, por ejemplo).

Para alcanzar esta solución, es necesario tener una red que permita tecnologías de redireccionamiento transparentes, como el Web Cache Communication Protocol (WCCP, protocolo de comunicación del caché Web). Con está tecnología, las caché de la red se agregan a ubicaciones clave en la red para lograr la solución de localización del tráfico. Las caché de la red almacenan el contenido al que se tiene acceso con frecuencia y después lo sirve localmente para entregar solicitudes para el mismo contenido, pero sin tener que regresar a Internet o WAN para obtenerlo. Obviamente, esto alivia la congestión porque no tienen que volver a enviarse transmisiones repetidas. En la figura 11-6 se ilustra este proceso:

1. Al usar un navegador Web, un usuario solicita una página Web.
2. La red examina esta solicitud y después la redirige a un caché de red local. Esto se hace de manera transparente, de modo que el usuario no está consciente del redireccionamiento.
3. Tal vez la caché no tenga la página Web almacenada. En ese caso, la caché hace su propia solicitud del servidor Web original.

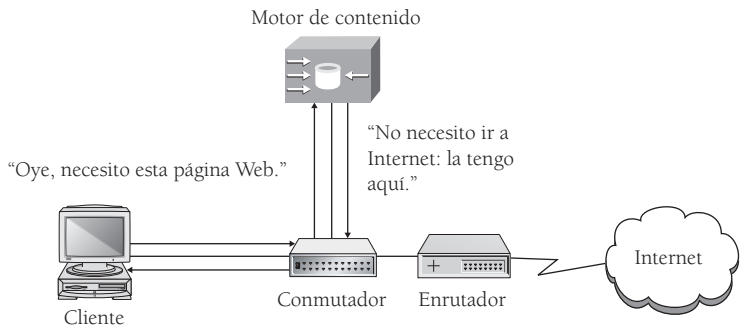


Figura 11-6. Las páginas Web a las que se tiene acceso frecuente se almacenan de forma local en caché.

4. El servidor Web original entrega la pagina Web solicitada a la caché, que después la reenvía al usuario. La caché almacena una copia de la página en caso de que se necesite después.
5. Cuando otro usuario solicita la misma página Web, esta vez la caché tiene la página a la mano y la solicitud se satisface de forma local.
6. La entrega la página Web al usuario de forma local. Esto elimina la necesidad de usar ancho de banda WAN y entrega el contenido mucho más rápido.

Protocolo de comunicación de la caché de Web

Aunque ya mencionamos varios protocolos CDN en este capítulo, el protocolo propiedad de Cisco para permitir el almacenamiento en caché transparente a través de una red (Web Cache Communication Protocol, WCCP) se ha convertido en el protocolo sobre el que están construidas las soluciones de Cisco. Este protocolo usa las redirecciones HTTP para proporcionar funcionalidad. La primera versión de WCCP sólo permitía la comunicación con un enrutador, no soportaba la transmisión múltiple y estaba limitada al tráfico HTTP. La versión actual es WCCP v2 y resuelve las deficiencias de la versión 1.

WCCP usa el puerto 2048 UDP, que opera a través de un túnel de Generic Routing Encapsulation (GRE, encapsulamiento de enrutamiento genérico) entre el enrutador y el motor o los motores de contenido. Una vez que se ha entregado el contenido, ya sea mediante el motor de contenido o el servidor Web de origen, los paquetes HTTP son entregados sin modificaciones.

Los motores de contenido mantienen una lista de enrutadores con los que tienen comunicaciones WCCP. Cuando el motor de contenido se identifica ante los enrutadores, éste comparte su lista de enrutadores. A cambio, los enrutadores responden con una lista de motores de contenido que ven en el *grupo de servicio*. En cuanto todos los dispositivos se reconocen entre sí, un motor de contenido se convierte el motor líder y determina de qué manera se redireccionarán los paquetes.

Los motores de contenido envían *latidos* a los enrutadores cada diez segundos a través de un túnel GRE. Si hay un grupo de motores de contenido y uno de los motores no envía un latido en 30 segundos, el enrutador informa al motor de contenido líder que el motor está desaparecido y sus recursos tienen que reasignarse a los motores restantes.

NOTA Hablaremos más acerca de recursos específicos en un grupo y lo que significa un grupo en páginas posteriores de este capítulo.

Actualización

Una preocupación obvia cuando se utiliza el almacenamiento en caché es el tema de la actualización. ¿Cómo puede estar seguro de que la página que está buscando contiene la información más actual? Es decir, ¿qué evita que el motor de contenido almacene a perpetuidad la visita al sitio Web de la página del periódico del viernes pasado?

Cada página Web está integrada por varios objetos Web, y cada objeto tiene sus propios parámetros de almacenamiento en caché que son establecidos y administrados por los autores de la página Web y los estándares HTTP. Así, por ejemplo, nuestro sitio Web del periódico tendrá contenido nuevo, pero cosas como barras de herramientas, botones de navegación y el membrete pueden almacenarse en caché. Como tal, cuando el motor de contenido almacena el sitio Web del periódico, incluye los elementos que es probable que no cambien, después sale para obtener el contenido nuevo. Los motores de contenido entregan contenido actualizado al obedecer los estándares de caché HTTP (de los que hablaremos en un momento) y permitir a los administradores decidir cuándo debe actualizarse el contenido desde los servidores Web de origen.

Los autores Web pueden establecer hasta qué grado permitir el almacenamiento en caché. En HTTP, es posible administrar los parámetros de almacenamiento en caché para cada objeto en un sitio Web. El contenido puede configurarse para almacenar en el caché de acuerdo con tres opciones:

- ▼ El contenido no puede almacenarse en caché.
- ■ El contenido puede almacenarse en caché (la opción predeterminada).
- ▲ El contenido puede almacenarse en caché, pero expirará en una fecha determinada.

HTTP 1.1 introdujo un mecanismo de actualización llamado If-Modified-Since (IMS), que asegura que los datos almacenados en caché estén al día. Los motores de contenido envían una solicitud IMS a un servidor Web de destino cuando el motor recibe una solicitud de un contenido que ha expirado en el caché o cuando recibe solicitudes IMS de clientes donde un contenido en el caché es más antiguo que un porcentaje de su edad máxima. Si el contenido en el servidor Web de destino determina que el contenido en el motor no se ha actualizado, envía un mensaje al motor de contenido para que siga adelante y sirva los datos almacenados al cliente. Si el contenido ha sido actualizado y no es reciente, el motor de contenido recuperará el nuevo contenido.

Pero la actualización no está sólo en las manos de los creadores de páginas Web. Los administradores de red pueden controlar la actualización de objetos Web en sus motores de contenido. Los motores de contenido tienen un parámetro llamado *factor de actualización*, que puede ser configurado por parte de un administrador de red. Esto sólo determina la

rapidez con la que expira el contenido. Cuando un objeto se almacena en caché, se calcula un valor TTL. Ese valor es:

TTL = (fecha actual – fecha de la última modificación) * factor de actualización

Si el contenido ha expirado, con base en la formula mencionada, los datos Web se actualizan en caché la próxima vez que se emita una solicitud IMS.

Para establecer una directiva de actualización modesta, el factor de actualización puede configurarse en un valor bajo (más o menos .05), para que el objeto expire más rápido. Sin embargo, esto causará más consumo de ancho de banda a medida que se actualizan las páginas. Configurar el factor de actualización a niveles más altos causará menos consumo de ancho de banda.

NOTA La actualización también puede ser administrada por el cliente. Éste puede hacer clic en el botón Reload o Refresh del explorador. Esto causará una serie de solicitudes IMS preguntando por los objetos Web que se han actualizado. Como opción, MAYÚS-RELOAD o MAYÚS-REFRESH causa que se pase por alto a los motores de contenido y que el contenido se envíe directamente al cliente desde el servidor Web.

Almacenamiento en caché de los motores de contenido

Existen tres maneras diferentes en el que el contenido puede almacenarse en caché en una solución Cisco: transparente, estilo proxy y estilo proxy inverso. La manera más común de almacenar en caché es el estilo transparente. Sin embargo, también es útil entender los otros métodos, porque pueden ser más relevantes y útiles para las necesidades de su organización.

Almacenamiento transparente en caché

El primer método es conocido como almacenamiento transparente en caché. Ya describimos los pasos relacionados con este tipo de almacenamiento en caché (en esencia, un navegador Web solicita una página Web). Esa solicitud se ejecuta primero a través de un enrutador WCCP habilitado, donde se analiza. Si el enrutador determina que un motor de contenido local tiene el contenido deseado en caché, ésta envía la solicitud al motor de contenido, que entrega el contenido de vuelta al navegador. Si no está en caché, el motor de contenido va a Internet para traer y almacenar la página.

Debido a que este método usa un enrutador WCCP habilitado, el motor de contenido trabaja de manera transparente con el navegador. No debe configurarse a los clientes para señalar a un caché de proxy específico. Como el motor de contenido es transparente a la red, el enrutador actúa en una función "normal" para el tráfico que no tiene que ser redirigido.

Sin embargo, al usar un conmutador CSS, la solicitud del cliente nunca llega al enrutador. En despliegues más grandes, cobra mayor sentido tener un conmutador CSS para tomar decisiones acerca de si un contenido en particular ya se ha almacenado en caché de forma local. Además, es probable que los despliegues grandes necesiten varios motores de contenido y los datos se almacenarían en cada dispositivo, con base en un Uniform Resource Locator (URL, localizador uniforme de recursos).

HTTPS Todo el proceso de almacenar en caché parece muy sencillo, en especial si alguien solicita contenido estático. Sin embargo, hay gran cantidad de contenido en Internet, en su

intranet o posiblemente al atravesar un vínculo WAN dinámico. Por ejemplo, hay ocasiones en que la solicitud de una página Web hecha por el usuario tendrá que ir al servidor Web previsto.

El concepto de almacenar en caché no se tira por la ventana en estos caso. Consideremos qué pasa cuando se inicia una sesión de Secure HTTP (HTTPS, HTTP segura).

1. El usuario inicia una sesión HTTPS. Es tomada por el enrutador habilitado por WCCP y enviada al motor de contenido.
2. El motor de contenido, configurado como servidor HTTPS, recibe la solicitud del enrutador.
3. El motor de contenido obtiene un certificado de Secure Sockets Layer (SSL, capa de conexiones seguras) del servidor Web de destino y se envía de regreso al cliente (a través del motor de contenido) para que negocie la conexión SSL.
4. El cliente envía las solicitudes HTTPS dentro de la conexión SSL.
5. El motor de contenido analiza la solicitud. Si la información está en su caché, el proceso de solicitud HTTP ocurre. Si el contenido se encuentra en caché del motor de contenido (a lo que se le conoce como *visita al caché*), éste envía de regreso el contenido deseado usando la conexión SSL.
6. Si el contenido no está almacenado dentro del motor de contenido (a lo que también se le conoce como *falta en caché*), establece una conexión con el servidor Web de destino y solicita el contenido a través de la conexión SSL.
7. Si es posible, el motor de contenido almacenará en caché la información y enviará una copia de regreso al cliente a través de una conexión SSL.

Omisión del contenido Existen ocasiones en que el motor de contenido simplemente tiene que ser evitado para conseguir la sesión que el cliente necesita. Aunque existen mecanismos para establecer sesiones HTTPS, no todas las conversaciones seguras pueden ser aceptadas a través del motor de contenido.

Algunos sitios Web dependen de la autentificación y, como tal, no permiten que el motor de contenido se conecte en nombre del usuario. Los motores de contenido pueden usar la omisión de la autentificación de tráfico para evitar la interrupción del servicio. La omisión del tráfico de autentificación se usa automáticamente para crear una lista de acceso dinámico para los pares cliente/servidor.

Cuando un par cliente/servidor va dentro de la omisión de autenticación, se omite por un lapso determinado. La configuración predeterminada es de 20 minutos, pero ese valor puede cambiarse, dependiendo de las necesidades de la organización.

Almacenamiento en el caché transparente/estilo proxy

El almacenamiento en caché no transparente o *estilo proxy* es conocido para el cliente, mientras que el almacenamiento transparente ocurría sin el conocimiento del cliente de lo que estaba ocurriendo. Con el almacenamiento en caché de proxy, la caché del proxy realiza una búsqueda DNS en nombre del cliente. Los proxies se usan en diferentes protocolos, como HTTP, HTTPS, FTP, etcétera. Considere la red que se muestra en la figura 11-7.

El cliente ha sido configurado para usar un servidor proxy para las solicitudes HTTP. Por lo general, se usa el puerto 8080, pero pueden configurarse diferentes puertos para el protocolo que desea administrar.

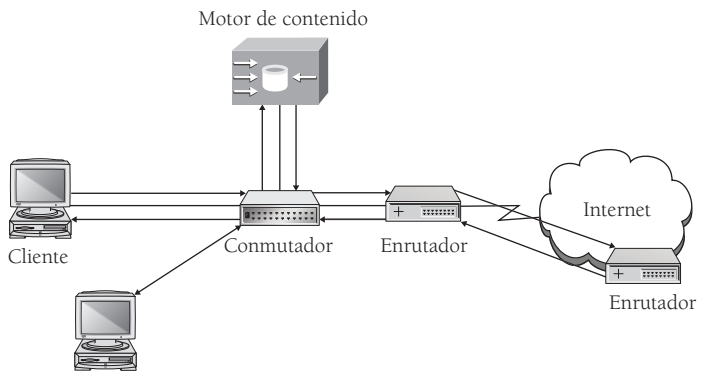


Figura 11-7. El almacenamiento en caché estilo proxy funciona en nombre del cliente.

La dirección IP del proxy también se configura en el cliente. En el ejemplo, estamos utilizando la dirección 10.1.100.100. Sigamos este método de almacenamiento en caché paso a paso:

1. Las solicitudes HTTP para el contenido son dirigidas al proxy.
2. Si el caché del proxy no tiene el contenido, el proxy realiza una búsqueda DNS del sitio Web de destino.
3. Cuando el DNS ha sido resuelto, el proxy solicita el contenido del servidor Web de destino y luego lo recupera.
4. El contenido se almacena en caché antes de enviarse al cliente. Esto asegura que la próxima vez que se solicite el contenido, el caché lo tendrá.

El almacenamiento en caché de proxy es útil porque el caché puede estar en cualquier lugar de la red. Además, se proporciona una medida de seguridad de red para que sólo el cliente se ponga en contacto con el proxy, de modo que las reglas del firewall pueden ser más estrictas, permitiendo que sólo el proxy pueda trabajar a través del firewall.

Almacenamiento en caché de proxy inverso

En el método proxy que ya se mencionó, el servidor proxy es un proxy para el cliente. En el método de proxy inverso, el servidor proxy actúa como proxy del servidor. Este método también almacena el contenido seleccionado, mientras que los métodos transparentes y de proxy, almacenan el contenido solicitado con frecuencia.

Existen dos casos en que es deseable el método de almacenamiento en caché de proxy inverso:

- ▼ La réplica del contenido para ubicaciones geográficamente dispersas.
- ▲ La réplica del contenido para equilibrio de carga.

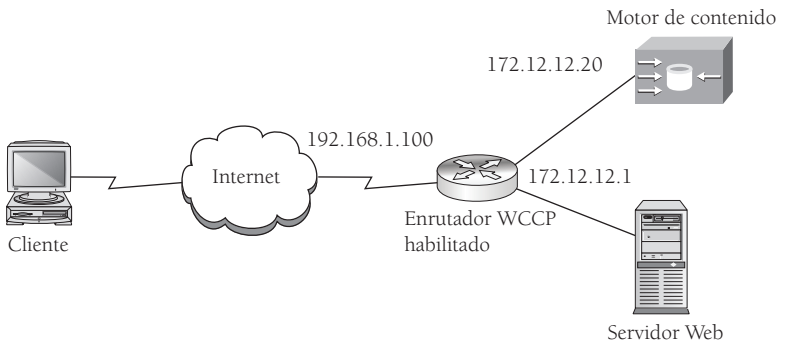


Figura 11-8. El almacenamiento en caché de proxy inverso con enrutadores WCCP habilitados coloca al motor de contenido enfrente del servidor Web.

En este escenario, el servidor proxy está configurado con una dirección IP enrutable para Internet. Es decir, los clientes van al servidor proxy con base en la resolución DNS de un nombre de dominio.

Servidores WCCP Considere el despliegue del caché que se muestra en la figura 11-8. El motor de contenido trabaja con un enrutador WCCP habilitado y se configura para el servicio proxy inverso para un servidor Web. En este escenario, la interfaz del enrutador vinculada con Internet tiene una dirección IP de 192.168.1.100. Las solicitudes HTTP enviadas a este servidor se envían primero a la interfaz del enrutador en 172.12.12.1. Una vez que la solicitud HTTP ha sido recibida en esta interfaz, el enrutador la redirige al motor de contenido (con una dirección IP de 172.12.12.20). En este caso, el motor de contenido está enfrente del servidor Web, ayudando a reducir la cantidad de tráfico en éste. Si la información solicitada no está en el motor de contenido, éste envía una solicitud al servidor Web local del contenido.

Conmutadores CSS Considere el despliegue de la caché que se muestra en la figura 11-9. Aquí, el motor de contenido se despliega con un enrutador WCCP habilitado y un conmutador CSS. Un usuario envía una solicitud para el contenido de la página Web. Ésta se acepta en la dirección IP virtual del conmutador CSS. Cuando el conmutador CSS toma una solicitud, la remite al motor de contenido. Si éste no tiene los datos solicitados, reenviará una solicitud al servidor Web.

Despliegue de varios motores de contenido

Los motores de contenido pueden estar localizados en varios puntos a través de una organización para un rendimiento óptimo del almacenamiento en caché. Por ejemplo, considere la organización que se muestra en la figura 11-10. En este caso, la organización es servida por tres motores de contenido. El primero maneja el almacenamiento en caché para el departamento de servicios al cliente en las oficinas centrales de la organización; el segundo maneja el almacenamiento en caché para el departamento de producción en una sucursal.

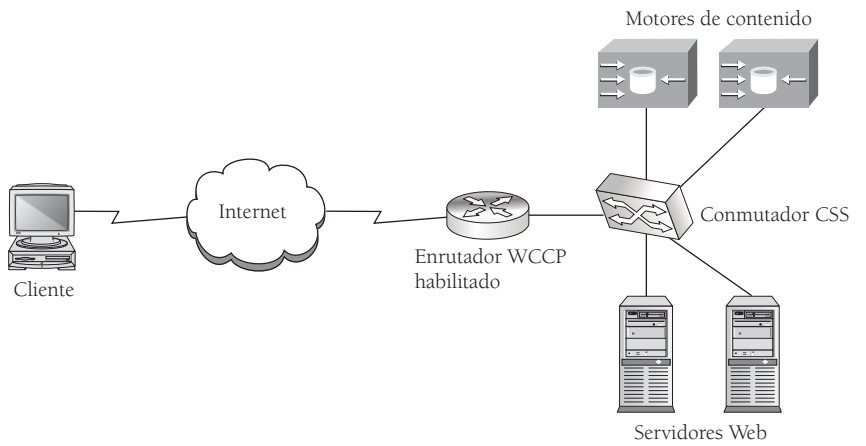


Figura 11-9. En un escenario de proxy inverso con conmutadores CSS, se revisan primero los motores de contenido antes de remitir la solicitud al servidor Web.

Si el cliente en el departamento de servicios al cliente envía una solicitud de página Web que puede ser acomodada por el primer motor de contenido, será servida por ese dispositivo. Si ese motor de contenido no puede satisfacer la solicitud, la envía al servidor Web de extremo. Antes de llegar al servidor Web de destino, la solicitud es considerada por el motor de contenido en el principal punto de acceso a Internet.

Esto proporciona otra oportunidad para que el contenido sea servido antes de tener que salir a Internet o a una WAN. Si este motor de contenido puede satisfacer la solicitud, entonces es innecesario que vaya a Internet. Si alguien de la sucursal ha solicitado la página,

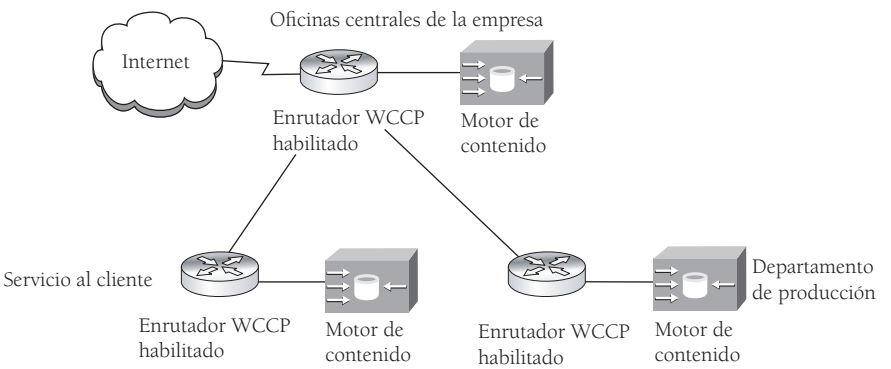


Figura 11-10. Los motores de contenido en diferentes niveles de una organización posibilitan una mayor disponibilidad del contenido.

tal vez esté almacenada aún en el motor de contenido número tres, en las oficinas centrales de la empresa.

Este escenario es muy útil para los proveedores de servicio de Internet. Con un motor de contenido sirviendo a varios clientes, en caso de solicitarse sitios Web comunes, es innecesario seguir recibiendo la página de Internet. En cambio, el motor de contenido puede servirla localmente.

Agrupamiento

Otra manera de administrar los niveles elevados de tráfico es el agrupamiento. Esto significa simplemente que varios motores de contenido se configuran juntos. Por ejemplo, un motor de contenido 7325 de Cisco, puede soportar más de 155 Mbps de tráfico y hasta 936 GB de datos. Sin embargo si se añade un segundo 7325, entonces el grupo puede manejar más de 310 Mbps de velocidad de transmisión de datos y 1.87 TB de datos. Es posible agrupar hasta 32 motores de contenido.

Cuando se agrega un nuevo motor al grupo, el enrutador habilitado con WCCP detecta el nuevo dispositivo y reasigna los recursos para el nuevo motor de contenido.

Los motores de contenido usan los llamados *contenedores*. Los enrutadores habilitados con WCCP redirigen el tráfico a los motores de contenido con el uso de un procedimiento de desmenuzamiento basado en la dirección IP de la solicitud entrante, y la solicitud se envía a uno de 256 contenedores. Al usar una técnica de desmenuzamiento, las solicitudes se esparcen de manera uniforme entre todos los 256 contenedores y, por tanto, a todos los motores de contenido del grupo.

Cuando se agrega un motor de contenido nuevo al conjunto, el enrutador habilitado con WCCP detecta el nuevo motor, y después se reconfigura el número de contenedores, con base en el número total de motores de contenido. Por ejemplo, digamos que su organización tiene dos motores de contenido. Cada motor contendrá 128 contenedores. Si se agrega un tercero, entonces cada motor se reconfigura para que contenga 85 u 86 contenedores.

Sin embargo, debido a que un motor de contenido nuevo no tendrá ningún contenido cuando se agregue, éste sufrirá faltas frecuentes en caché hasta que haya construido su almacenamiento. Este problema se aminora inicialmente porque el nuevo motor de contenido envía un mensaje a los otros en el grupo, buscando el contenido solicitado. Si otro motor del grupo tiene el contenido, se enviará al nuevo motor. Una vez que el motor decida que tiene el contenido suficiente de sus cohortes (con base en parámetros establecidos por el administrador de red), éste dejará de molestar pidiendo a sus pares las solicitudes de contenido y en cambio le preguntará al servidor final.

Confiabilidad

El agrupamiento no es sólo una buena manera de crear un equilibrio de carga de almacenamiento en caché de las solicitudes, también es una buena manera de asegurar la confiabilidad. En caso de que deje de funcionar uno de los motores de contenido del grupo, el enrutador habilitado con WCCP entra en juego y redistribuye la carga de ese motor entre los motores restantes. El sistema sigue operando, pero con un motor de contenido menos. Ciertamente, esto no es ideal para un punto de inicio confiable, pero al menos el sistema permanece accesible hasta que se restaure el motor de contenido que ha fallado.

Si falla todo el grupo, entonces el enrutador habilitado con WCCP se dejará de preocupar por almacenar en caché, mandando las solicitudes Web a sus servidores Web de

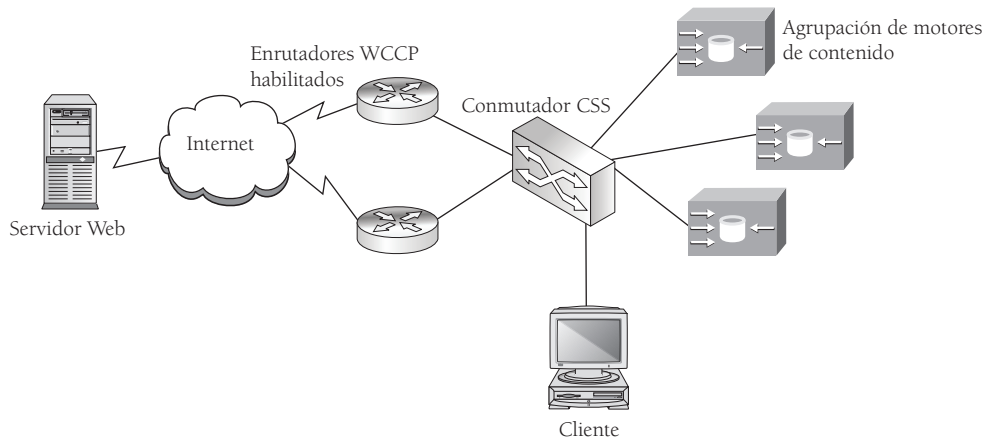


Figura 11-11. Multihoming proporciona confiabilidad, además de equilibrio de carga.

destino. A los usuarios finales sólo les pasará por la mente que está tardando más en llegar el contenido Web.

Al parecer, como tal vez ya lo habrá notado, se ha colocado una gran responsabilidad sobre los hombros del enrutador habilitado con WCCP. Si un motor de un grupo deja de funcionar, es fácil redistribuir la carga a otros dispositivos. Pero ¿qué pasa si falla el enrutador habilitado con WCCP? En ese caso, y suponiendo asumiendo que las piezas están en su lugar antes de una falla, un enrutador habilitado con WCCP, que ejecuta el Multigroup Hot-Standby Router Protocol (MHSRP, protocolo de enrutador activo en espera de grupos múltiples) proporciona protección de enrutamiento. A este enrutador se le conoce como *WCCP multihoming* (WCCP multirretorno).

Considere la red que se muestra en la figura 11-11. Hay dos enrutadores habilitados con WCCP. En el caso de que uno de estos enrutadores falle, el otro saldrá a remplazar a su hermano, redirigiendo las solicitudes Web al grupo del motor de contenido. La red que se muestra en la figura 11-11 es totalmente redundante, porque emplea ambos, una agrupación de motor de contenido y WCCP multihoming.

Omisiones

Multihoming y agrupamientos son buenas maneras de planear para evitar problemas. Sin embargo, a pesar de ser tan efectivos, no son perfectos. Tal vez exista una situación en que tenga que evitarse todo el sistema de caché. Existen dos escenarios en que se evita el sistema de caché.

Sobrecarga La omisión de la sobrecarga se usa cuando hay una oleada de tráfico Web y el motor de contenido o el grupo terminan simplemente abrumados. Cuando esto ocurre, el motor de contenido es capaz de percibir cuando hay una sobrecarga y rechaza las solicitudes adicionales hasta que pueda manejar las que ya están reservadas. Por tanto, las solicitudes

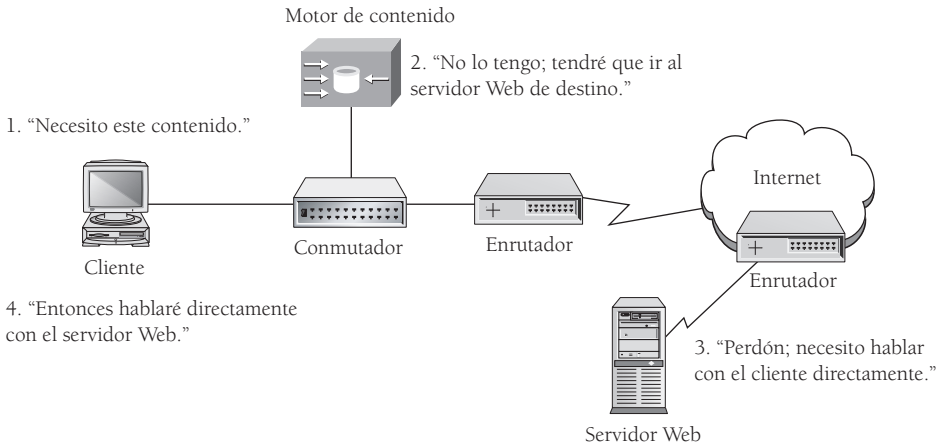


Figura 11-12. Si es necesario, el cliente puede evitar la infraestructura de almacenamiento en caché e ir directamente al origen.

Web entrantes simplemente se remiten a los servidores Web de destino, sin importar si el contenido está almacenado en el motor de contenido. Éste sigue rechazando solicitudes hasta que determine que no sólo se ha prevenido la situación de sobrecarga, sino que no volverá a sobrecargarse si toma nuevas solicitudes.

Si el motor de contenido está tan asediado con las solicitudes que no puede comunicarse con el enrutador habilitado con WCCP y compartir mensajes de estado, el enrutador removerá de forma lógica el motor del grupo, reasignando sus contenedores a otros motores del grupo.

Cliente Si un cliente necesita ser autentificado en el sitio Web usando la dirección IP del cliente, la autentificación fallará si se ve la dirección IP del motor de contenido en lugar de la del cliente. En esos casos, el motor de contenido permitirá al cliente omitir el motor y conectarse directamente con el servidor Web de destino.

Considere el intercambio que se muestra en la figura 11-12. En esta figura, el cliente intenta acceder a un servidor Web que insiste en la autentificación. En primer lugar, la solicitud se concentra a través del motor de contenido. Al ver que la información no está almacenada localmente, se remite al servidor Web de destino. Si se regresan códigos de error al motor de contenido (por ejemplo, un 401-unauthorized o 403-forbidden), el motor pasará automáticamente al modo de omisión para el cliente y permitirá que el cliente interactúe directamente con el servidor Web de destino. Además, el motor de contenido almacenará la dirección IP del destino junto con la del cliente. La próxima vez que el cliente intente acceder al servidor Web, el motor de contenido automáticamente entrará en el modo omisión para el cliente.

Si piensa que los días dorados de la interconectividad ya quedaron atrás, no ha visto nada todavía. El futuro es brillante, a medida que las tecnologías y protocolos son capaces de manejar más y más. A medida que las redes se vuelven más inteligentes, podemos es-

perar más servicios, con una especial atención dedicada a las condiciones de la red y las necesidades específicas del contenido.

SOLUCIONES DE VIDEO DE CISCO

Aunque "contenido" en las redes de entrega de contenido puede significar cualquier tipo de datos, estas redes están bien adaptadas para la entrega de video. Tiene sentido: el contenido de video y multimedia es muy grande, y muchos de estos contenidos necesitan entregarse a velocidades que permitan verlos en tiempo real. En esta sección se examinan las soluciones de video de Cisco. Pero antes de adentrarnos en cosas específicas, echemos un vistazo a lo que significa la adquisición de Scientific-Atlanta por parte de Cisco en 2005 para las soluciones generales de productos de video para la compañía.

Scientific-Atlanta

Como se mencionó en el capítulo 1, Cisco ha hecho adquisiciones muy importantes. Tal vez la mayor haya ocurrido en noviembre de 2005 con su compra por seis mil 900 millones del fabricante de sintonizadores de televisión por cable Scientific-Atlanta.

Hasta 2003, las adquisiciones de Cisco giraban alrededor de las tecnologías que eran útiles en centros de datos y clóset de cableado (equipo que la mayoría de los consumidores probablemente nunca verán). Sin embargo, en 2003, Cisco compró el grupo Linksys, un creador de enrutadores, conmutadores y aplicaciones WiFi enfocadas a los consumidores. Con el éxito de negocios que significó esa adquisición, Cisco ha estado buscando nuevos lugares para plantar su bandera. La adquisición de Scientific-Atlanta promete llevar a Cisco a muchos hogares, porque esta compañía domina el mercado de televisión por cable con un aproximado de 50% de participación de mercado. Pero antes de que se preocupe por tener un logo de Cisco tatuado en su cuello con un número de serie debajo, el dominio mundial de Cisco aún no lo ha apresado.

Dicho esto, ésta adquisición es un movimiento importante para Cisco.

Crecimiento y estancamiento

Durante la década de 1990, las ventas de Cisco tuvieron un gran despegue. La generación de Internet necesitaba su infraestructura, y Cisco proporcionó todos los bloques de construcción. Sin embargo, cuando llegó el milenio, todos tenían la infraestructura que necesitaban y la burbuja punto com explotó. Ahí fue cuando las ventas de Cisco parecieron estancarse. Para recuperar sus ventas (y mantener a los accionistas felices), Cisco necesitaba encontrar nuevas personas para que compraran sus productos. Así que entró al mercado para el consumidor.

Cisco no puso todos sus huevos en una sola canasta del lado del consumidor. También se están concentrando en las comunicaciones de emergencia para quienes responden las llamadas, pequeños negocios y soluciones inalámbricas. Pero la mayor venta viene potencialmente del consumidor casero.

Al entrar al mercado de video, Cisco puede dar la bienvenida a 10 mil millones para el 2009.

Oportunidad

Con toda la convergencia de las compañías de cable, de teléfono y parecidas, ha existido una demanda de redes que pueden entregar todo tipo de tráfico digital a través de una red IP. Estas compañías están peleándose por proporcionar servicios de acceso a Internet, teléfonos IP, servicios inalámbricos y de video, en un solo cable. Cisco estaba en una buena posición con las tres primeras, pero carecían de alguna forma de los servicios de video. Sin embargo, con la compra de Scientific-Atlanta, Cisco se encuentra en una buena posición para convertir todo eso en dinero en efectivo.

Cuentas de negocio

El potencial para los productos de servicio de video de Cisco no está totalmente orientado hacia los consumidores. Después de todo, también el proveedor de servicio necesita equipo en su extremo. Cisco ya vende casi mil millones de dólares en equipo a las compañías de cable cada año. Sin embargo, la compra de Scientific-Atlanta le permite vender productos en todos los puntos de la cadena: desde enrutadores que canalizan el tráfico de Internet hasta las antenas de Scientif-Atlanta, que llevan el contenido de los satélites a los sintonizadores de TV.

Tal vez algunas compañías de cable no tengan ganas de ir con un distribuidor por su equipo, pero una compañía como Cisco es capaz de introducir rápidamente equipo rico en características. Esto dará más opciones a los consumidores, y es probable que abran un poco sus chequeras cuando sea el momento de suscribirse a servicios adicionales.

Áreas intermedias

Hasta este punto, el mundo de Cisco ha girado primordialmente alrededor del hardware. A medida que los medios convergen con la computación y los teléfonos caseros, Cisco se puede encontrar pisando el césped de otras compañías (Microsoft incluida).

En el 2005, Cisco compró una compañía llamada KiSS, que fabrica reproductores DVD para Internet. Si Cisco logra combinar esta tecnología con sus nuevos sintonizadores para TV por cable (sin mencionar su tecnología inalámbrica de Linksys), permitirá a los consumidores copiar espectáculos en DVD y hacer transmisiones a otras PC y televisiones desde casa.

Por ejemplo, considere lo que Microsoft no ha podido lograr en el área de software de sintonizadores, a pesar del considerable esfuerzo. Esto es en mayor parte porque Scientific-Atlanta y Motorola (el otro gran productor de sintonizadores) tienen su propio software. Como tal, Microsoft ha volteado su atención relacionada con IP/TV a las compañías de teléfono, en vez de las de cable. Ya que el mercado de las telecomunicaciones IP/TV es más pequeño que el de las compañías de cable, la entrada de Cisco al mundo de IP/TV es un riesgo grande.

El tiempo dirá si la compra de Scientific-Atlanta le hará ganar dinero y llevará al dominio mundial que Cisco ha esperado, pero tiene un muy buen expediente con este tipo de cosas.

Solución de video para negocios de Cisco

Cisco no necesitaba a Scientific-Atlanta para entregar video a través de redes computacionales. Cisco tiene varias soluciones de video que cumplen con las diversas necesidades de entrega de contenido de video, empezando por su Cisco Business Video Solution.

La Cisco Business Video Solution no está limitada sólo para negocios. Escuelas y otras organizaciones se pueden beneficiar también de las opciones de videoconferencia de esta solución. Por ejemplo, una escuela puede usar esta solución para servir video bajo pedido

y cursos Web, aliviando así la necesidad de mantener una biblioteca de cintas de video y haciendo posible el aprendizaje las 24 horas.

La Cisco Business Video Solution se basa en la tecnología ACNS y está dirigida a organizaciones de cualquier tamaño que quieran extender información a empleados, consumidores, estudiantes, compañeros o cualquiera que necesite contenido multimedia.

Entre las características de la solución de video para negocios de Cisco se incluyen:

- ▼ **Acceso desde cualquier computadora** Empleados, consumidores, estudiantes y cualquier persona que necesite contenido pueden acceder a esa información desde cualquier computadora conectada a Internet.
- ■ **Fácil creación de contenido** Una herramienta de autoría basada en Web que permite que el contenido se entregue y despliegue de manera rápida.
- ■ **Integración** Se pueden sincronizar video y medios, junto con otros documentos, para proporcionar un entorno rico en multimedia.
- ■ **Contenido de varias fuentes** El contenido puede seleccionarse de varias fuentes de medios, incluidas VCR, DVD, alimentaciones de satélites y archivos de medios digitales, y después pueden codificarse en varias velocidades de bits dentro de archivos de Windows Media Player.
- ■ **Indización** El contenido de audio y video se indiza, con etiquetas que contienen la información de cada paquete de contenido, permitiendo la localización fácil del contenido.
- ■ **Facilidad de administración** El contenido es administrado por un sistema de administración activo central.
- ▲ **Facilidad de acceso** La solución está basada en un portal Web que proporciona acceso a un catalogo del contenido y acceso a las aplicaciones para autoría de contenido en vivo y VoD.

La Cisco Business Video Solution incluye estos componentes:

- ▼ **MediaPlatform Enterprise** Autoría y administración de contenido y entrega a través de MediaPlatform Enterprise, que facilita la creación, administración y distribución de contenido de video bajo pedido y en vivo. Esta herramienta utiliza una interfaz basada en Web, incluidas captura de audio y video, sincronización con diapositivas y otras imágenes de Microsoft PowerPoint, y edición HTML.
- ■ **Estudio** Una sugerencia de cuenta de materiales, implementación y despliegue para la operación sencilla de captura de audio y video.
- ■ **Portal Web** Una interfaz Web con herramientas necesarias para ver, crear y producir contenido VoD.
- ■ **Entrega en red** Para desplegar una solución VoD de negocios, es necesario incluir una red estructurada apropiadamente. Con ACNS de Cisco, el contenido de video y audio de elevado ancho de banda puede hacerse más accesible mientras se reducen las limitaciones de ancho de banda en la red.
- ▲ **Planeación, implementación y guías de operación** Estas guías son despliegues y experiencias de las mejores prácticas de Cisco que incluyen el conocimiento necesario para crear, desplegar y administrar el flujo de contenido de audio y video.

Solución de videoconferencia IP

En el capítulo 9 hablamos del sistema Cisco Unified Communications, un sistema con el que Cisco intenta cambiar la faz de la comunicación de negocios. Como el sistema Cisco Unified Communications, el sistema Cisco Unified Videoconferencing utiliza el protocolo Skinny propiedad de Cisco, junto con el Session Initiation Protocol (SIP, protocolo de inicio de sesión) y H.323. Este sistema permite que el contenido de video se agregue a conversaciones de audio.

NOTA H.323 es un estándar para la comunicación multimedia en tiempo real y se explicó más a fondo en el capítulo 9.

El sistema central del sistema es la tecnología AVVID de Cisco. Examinemos AVVID más a fondo antes de explicar cuáles son los componentes que integran una solución Cisco Unified Videoconferencing.

AVVID

AVVID (Architecture for Voice, Video, and Integrated Data, arquitectura de voz, video y datos integrados) de Cisco, es la tecnología para comunicaciones de la compañía.

En el pasado, las videoconferencias requerían sistemas de red ineficaces para desplegarse. Muchas organizaciones todavía tienen esas tecnologías, que utilizan ISDN y el protocolo H.320. Sin embargo, con las redes Ethernet conmutadas, enrutadores de extremo alto y calidad de servicio capas 2 y 3, es más simple y barato desplegar la videoconferencia.

En la tabla 11-1 se explican los componentes principales de una solución de videoconferencia IP AVVID.

Productos de videoconferencia IP

Los productos de la familia Cisco Unified Videoconferencing incluyen varios sistemas modulares y apilables. Los productos son parte de la familia IP/VC de Cisco, casi todos construidos a partir de la serie IP/VC 3500 de Cisco. Esta serie incluye:

- **IP/VC 3510 MCU de Cisco** Permite a los participantes de diferentes lugares asistir a la misma videoconferencia con conectividad en tiempo real. Una unidad de escritorio o montable en rack que permite conferencias entre tres o más puntos, esta unidad permite llamadas de conferencia multimedia. El usuario puede escoger el modo, permitiendo hasta cuatro ubicaciones mostradas en la pantalla a la vez. Como opción, la conferencia puede usar un modo de conmutación, donde la pantalla muestre a la persona que está hablando o el moderador puede controlar qué persona se muestra en la pantalla. Este modelo MCU puede soportar hasta 15 participantes en anchos de banda de hasta 1.5 Mbps. Su diseño también permite a múltiples MCU estar vinculados para soportar videoconferencias más grandes. Despliegues más pequeños pueden beneficiarse de las funciones de portero incluidas.
- **IP/VC 3522 y IP/VC 3527 de Cisco** Son los dispositivos de escritorio y de rack que traducen entre los protocolo H.323 y H.320. Estos dispositivos son componentes importantes, si necesita conectar el sistema heredado H.320 a una nueva solución IP/VC.

Componente	Descripción
Terminal de video	La unidad con la que el usuario se familiariza más: unidades de escritorio y PC individuales o dispositivos de cuartos de conferencia.
Portero	Realiza la resolución de dirección, administración de ancho de banda, control de admisión de llamadas, administración de zona y enrutamiento de llamadas.
Gateway	Realiza traducciones entre varios protocolos (como SIP, Skinny y H.323), formatos de codificación de audio y de video usados por otros componentes.
Unidad de conferencia multipunto	Facilita que tres o más participantes se unan en una videoconferencia. Este dispositivo administra las funciones de control de llamada, recursos de conferencias y flujo de video y audio.
Proxy	Un agente de procesamiento de llamadas que termina las llamadas H.323 de una LAN local y establece sesiones con puntos finales en las LAN remotas.

Tabla 11-1. Componentes de una solución AVVID.

- El gateway IP/VC 3522 puede comprarse como un dispositivo de dos o cuatro puertos con una Basic Rate Interface (BRI, interfaz de tasa básica) o interfaces WAN V.35. Soporta hasta ocho llamadas a velocidades de hasta 64 Kbps (BRI).
- El gateway IP/VC 3527 utiliza Primary Rate Interface (PRI, interfaz de tasa principal) al PSTN, y es configurable con conexiones T1 y E1. Esta unidad soporta 23 llamadas en un T1 y 30 en E1.

Estos dispositivos también ofrecen funciones de portero incorporadas para redes de videoconferencia pequeñas.

- **IP/VC Video Terminal Adapter (VTA) de Cisco** Conecta un solo sistema basado en cuarto H.320 a una red IP. Es una unidad de escritorio o de rack, ofrece dos interfaces WAN V.35, señalación EIA/TIA-366 y un puerto Lan Ethernet, y opera a velocidades de hasta 768 Kbps.
- **Administrador de Conferencia Multimedia de Cisco** Es un portero/proxy H.323. Cuando estos productos se combinan con un punto final H.323 obediente, un sistema de videoconferencia completo es desarrollado.

Administrador de Conferencia Multimedia de Cisco Configurar y administrar una solución IP/VC es una función del Multimedia Conference Manager (MCM, administrador de conferencia multimedia), un componente del software IOS de Cisco.

Funciona como un portero y proxy H.323, permitiendo al administrador de red controlar las opciones de ancho de banda y calidad de servicio. El MCM está disponible en varios enrutadores, incluyendo las series 2500, 2600, 3600 y 7200 de Cisco.

Las funciones MCM del IOS pueden administrar:

- ▼ Puntos finales de videoconferencia.
- ■ Gateways de video H.320 y H.323.
- ■ Telefonía IP.
- ■ PBX IP.
- ▲ Gateways de telefonía PSTN-IP.

Las características avanzadas del subsistema MCM incluyen:

- ▼ Autentificación del usuario a través de RADIUS y TACACS+.
- ■ Connection Admission Control (CAC, control de admisión de conexión).
- ■ Asignación y administración de ancho de banda.
- ▲ Call Datail Records (CDR, registro detallado de llamadas).

Puntos finales Sus usuarios probablemente nunca verán un IP/VC 3540. Sin embargo, lo que usarán serán puntos finales: los clientes de una red de videoconferencia.

Cisco no fabrica puntos finales; sin embargo, sí trabaja con vendedores de puntos finales para asegurar la compatibilidad e interoperatividad.

En la figura 11-13 se muestra un ejemplo de un sistema de videoconferencia.

Sistema de medios digitales

Para administrar todas las soluciones que Cisco tiene para entrega de video, las organizaciones pueden voltear al Digital Media System (DMS, sistema de medios digitales) 3.3 de Cisco. DMS es una suite de aplicaciones que ayudan con la entrega y administración de contenido de video en vivo y bajo pedido. DMS consta de tres aplicaciones:

- ▼ Portal de video y herramienta de informes de Cisco.
- ■ Video Portal Manager (VPM, administrador del portal de video) de Cisco.
- ▲ onBusiness Network Content Library (biblioteca de contenido de red en negocios).

Echemos un vistazo más de cerca a estos componentes y cómo pueden ayudar a administrar las necesidades de video IP de su organización.

Portal de video de Cisco

El Cisco Video Portal usa una interfaz basada en red para permitirle entregar video en vivo y bajo demanda a sus espectadores, que son clientes, consumidores, empleados, estudiantes o cualquiera que sea la audiencia.

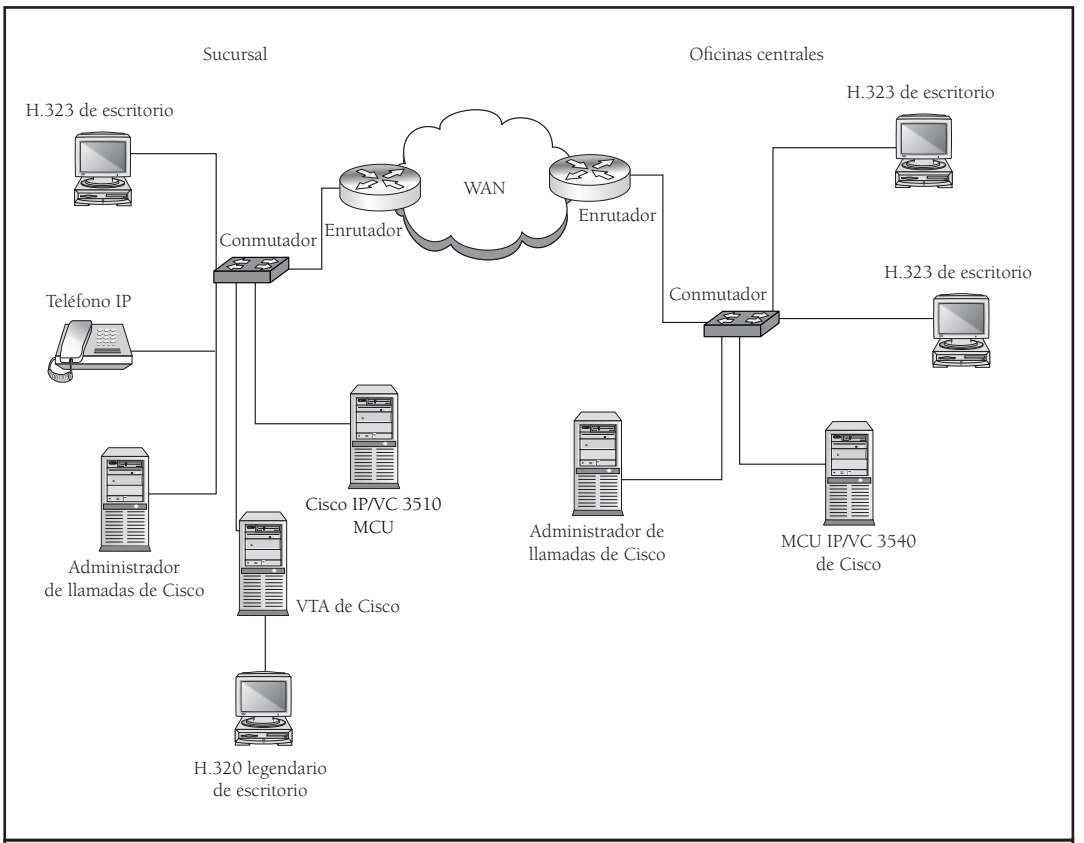


Figura 11-13. Una solución IP/VC usa componentes como Cisco CallManager, MCU, VTA y teléfonos IP.

El sistema se adapta a cualquier infraestructura de tecnología de la información, soportando formatos de video como Windows Media, Real y Flash. El portal de video incluye estas características:

- **Facilidad de búsqueda** El contenido puede encontrase de manera rápida por categoría, nombre o palabra clave.
- **Lista de reproducción personalizable** Los videos pueden ser enlistados dinámicamente por los autores del contenido o los usuarios.
- **Contenido complementario** Se puede agregar información adicional al video, incluidos marcadores, lectura adicional, contenido de medios relacionados, sitios Web y materiales descargables.

- **Reproducción y vista previa simultáneas** Puede verse una vista previa en miniatura mientras el video principal se está reproduciendo.
- **Acceso e informes** El uso del contenido puede ser seguido, monitoreado e informado.

Administrador del portal de video de Cisco

El siguiente componente de los sistemas de administración de video de Cisco es el Cisco Video Portal Manager (VPM). Como el portal de video de Cisco, VPM también es una aplicación basada en Web. Esta herramienta se usa para organizar y publicar video. Está diseñada para ayudar a los autores del contenido a subir, catalogar, editar, empaquetar y publicar sus propios contenidos de video al portal de video de Cisco.

VPM permite a los autores:

- Añadir y archivar el contenido.
- Asignar palabras clave de metadatos.
- Crear y administrar listas de reproducción.
- Crear y administrar contenido adjunto (como marcadores, mensajes, sitios Web y otros materiales descargables).
- Previsualizar contenido y administrar el flujo de trabajo.
- Programar entregas instantáneas y futuras.
- Administrar cuentas del administrador y permisos del usuario.

Biblioteca de contenido de red onBusiness

El componente final del sistema Cisco Video management no es tanto una aplicación o herramienta, sino que es un acceso a una biblioteca de video creada con anterioridad, producida por profesionales del medio, expertos de la industria y escuelas de negocios.

La onBusiness Network Content Library contiene diversos programas de video, incluidos títulos y temas como:

- Errores que cometen los administradores.
- Desarrollo de negocios.
- Planes y prácticas de comunicaciones eficaces.
- Ventas.
- Mercadotecnia.
- Cómo crean mercados las marcas.

Los CDN en general y los IP/TV en particular, proporcionan características ricas para una red. Ya sea que esté interesado en almacenar en el caché datos para que sean más fácil y rápidos de transmitir a los clientes o quiera desarrollar soluciones de video o videoconferencia, la base de cualquier esfuerzo será la CDN.

PARTE IV

Diseño de redes de Cisco

CAPÍTULO 12

Protocolos de enrutamiento

En los capítulos anteriores, cubrimos la amplia gama de dispositivos de red. Los conmutadores se instalan en un clóset de datos, utilizando cables de par trenzado desde los dispositivos host, formando una LAN, y también empacan el poder para soportar a las VLAN. Otro habitante del clóset de datos es el servidor de acceso, usado para vincular usuarios remotos en interconexiones a través de VPN de Internet o líneas de marcado telefónico. Si un paquete rebasa el segmento de LAN de origen, fluye a la LAN de espina dorsal, donde encuentra un enrutador y (si es una interconexión asegurada) un firewall. Después de ese punto se encuentra el más allá. Una vez que el paquete pasa la red local, entra en un reino de aparentemente infinita complejidad.

Las interconexiones son complejas porque son grandes y están sujetas a fluctuaciones sin fin. Una topología de interconexión se modifica cada vez que se agrega un nuevo conmutador o cuando se inserta un enrutador para ayudar a dirigir las cargas de interconexión crecientes. A medida que evolucionan los patrones de uso, la congestión de tránsito parece surgir cada día en diferentes puntos. Si los dispositivos de red dejan de funcionar, hacen que deje de funcionar el segmento de LAN con ellos, y el tráfico se debe redirigir de inmediato (y redirigirlo una vez más de regreso al dispositivo que dejó de funcionar en cuanto esté listo de nuevo). Lo más frecuente es que el dispositivo de red esté funcionando pero una de sus interfaces de red haya dejado de hacerlo, o que la interfaz esté bien, pero un cable se haya desconectado de su puerto por accidente. Por encima de todo esto, a veces el equipo de red físico está ejecutándose bien, ¡pero aún así las cosas no funcionan bien porque un archivo config dañado se introdujo de alguna manera en la mezcla!

Lo importante aquí es que las interconexiones grandes son simplemente demasiado complicadas para que los administre una sola persona. Imagine un cuarto lleno de administradores de red tratando de controlar manualmente todos y cada uno de los eventos de red en una de las compañías que aparecen entre las 500 más importantes del mundo de acuerdo con la revista *Fortune*, y tendrá un retrato de una desorganización que da escalofríos. Ahora imagine ese mismo cuarto (o incluso un edificio) lleno con gente que trata de acorralar al propio Internet, y verá un caos ilimitado. Hay demasiada complejidad y cambio por manejar sin una fuente constante de ayuda confiable (ayuda automatizada).

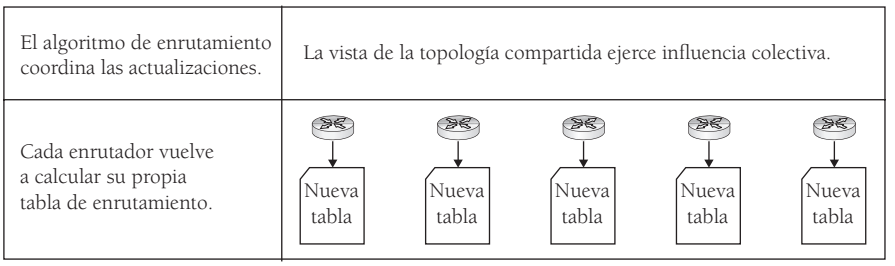
¿Cómo funciona todo? ¿Cómo encuentran los paquetes su camino entre las interconexiones con la confiabilidad que hemos llegado a dar por garantizada? La respuesta está en los protocolos de enrutamiento.

REVISIÓN GENERAL DE LOS PROTOCOLOS DE ENRUTAMIENTO

Como ya lo aprendió, un *protocolo* es un sistema formalizado para el intercambio de un tipo específico de información en una cierta manera, y un algoritmo es un sistema de reglas cuidadosamente diseñado para controlar un proceso que debe incluir varios factores.

En nuestro contexto, un *protocolo de enrutamiento* formaliza el intercambio constante de información de ruta entre enrutadores. Los mensajes llamados *actualizaciones de enrutamiento* pasan información usada por los algoritmos de enrutamiento para calcular rutas hacia los destinos. Un *algoritmo de enrutamiento* es un sistema de reglas que controla el comportamien-

to de una interconexión de tal manera que se adapta a las circunstancias cambiantes dentro de la topología de la interconexión. Los cambios constantes incluyen cosas como cuáles vínculos están activos y funcionando, cuáles son más rápidos, si apareció algún equipo nuevo, etcétera. Cada enrutador usa su propia copia del algoritmo para volver a calcular un mapa en la interconexión que valga para todos los últimos cambios desde su perspectiva particular.



Los protocolos de enrutamiento usan un acuerdo de igual a igual en que cada enrutador desempeña una función equitativa. Quienes son nuevos en el campo de las interconexiones a menudo consideran que los enrutadores son coordinados de alguna manera por un servidor de administración centralizado, tal vez un servidor SNMP. No lo son. No hay un servidor de protocolo de enrutamiento para administrar centralmente los procesos de enrutamiento. La actualización de la tabla de enrutamiento activa es manejada en tiempo real a través de una disposición en que cada enrutador toma sus propias decisiones de selección de ruta. Para configurar un protocolo de enrutamiento para una interconexión, el proceso de protocolo de enrutamiento debe estar configurado en cada enrutador que participará en la disposición. En términos prácticos, el archivo config del IOS de cada enrutador debe tener parámetros establecidos para enviar y recibir actualizaciones de enrutamiento, ejecutar el algoritmo, etcétera. Apropiadamente configurado, el protocolo de enrutamiento puede influir de manera colectiva en todas estas decisiones tomadas por la máquina, de manera que puedan funcionar en armonía. El área en que se intercambia la información de enrutamiento se denomina *dominio de enrutamiento*, o sistema autónomo.

Fundamentos del protocolo de enrutamiento

Entre los muchos protocolos de enrutamiento, algunos están basados en estándares y otros son de propietario. Varios son antiguos y su uso se está vetando, algunos sólo se usan dentro de nichos de mercado estrechamente definidos y otros tienen un uso tan amplio que son en realidad estándares *de facto*. Los protocolos de enrutamiento también difieren en el tipo de interconexiones para cuya administración están diseñados y en el tamaño de las interconexiones que pueden manejar. Como es natural, esta diferencia se manifiesta en cada algoritmo de protocolo de enrutamiento. Sin embargo, todos sus algoritmos comparten estos dos procesos básicos:

- ▼ Los enrutadores se envían mensajes de actualización entre sí, aconsejándose sobre los cambios en la topología y las condiciones de la interconexión.
- ▲ Cada enrutador vuelve a calcular sus propias tablas de enrutamiento con base en información actualizada.

La actualización mutua ayuda a cada enrutador individual a saber lo que está pasando. Lo que es más importante, ayuda a orquestar a los enrutadores de una interconexión al mantener un conjunto común de información con la cual operar.

La función central de la tabla de enrutamiento

Una *tabla de enrutamiento* es una lista de rutas disponibles para reenviar el tráfico a diversos destinos. Cada enrutador de una interconexión mantiene su propia tabla de enrutamiento, cuyo contenido difiere de los mantenidos por otros enrutadores. Cada enrutador mantiene una sola tabla de enrutamiento (no se mantiene una por interfaz). Casi todos los enrutadores ejecutan sólo un protocolo de enrutamiento, aunque los enrutadores de borde especializado ejecutan dos, para pasar las rutas entre las áreas que usan diferentes protocolos (veremos más sobre el tema en páginas posteriores de este capítulo).

NOTA Las tablas de enrutamiento a menudo consultan varias tablas para un protocolo de enrutamiento determinado. Por ejemplo, Open Shortest Path First (OSPF, abrir primero la ruta más corta) mantiene varias tablas de información que son parte de la tabla de enrutamiento.

Una tabla de enrutamiento constituye la visión centrada en el enrutador sobre la topología de la interconexión (una especie de fórmula personal para hacer negocios). Cada vez que se recibe una actualización, el protocolo de enrutamiento toma la información y la procesa con su algoritmo para volver a calcular las rutas óptimas a todos los destinos alcanzables desde ese enrutador. En la figura 12-1 se ilustra el proceso de actualización de la tabla de enrutamiento.

Cada enrutador debe tener su propia tabla de enrutamiento para incluir los puntos específicos de las condiciones de su ubicación en la interconexión. En un dominio de enrutamiento, los enrutadores comparten colectivamente las mismas noticias acerca de cualquier cambio, pero luego cada uno coloca la información para uso individual.

Los protocolos de enrutamiento son la inteligencia de las interconexiones

El objetivo de los protocolos de enrutamiento es dejar que una interconexión responda a los cambios. Lo hacen así al proporcionar enrutadores con un marco conceptual común para la toma de decisiones acerca de cómo responder a los cambios en la topología dentro de la interconexión. El protocolo de enrutamiento coordina el paso de las actualizaciones entre los enrutadores, y luego cada enrutador vuelve a calcular las rutas óptimas en su propia tabla. Si, después de volver a calcular, todas las tablas de enrutamiento han llegado a una lista común de topología (a pesar de que cada uno tiene su perspectiva) la interconexión ha llegado a la *convergencia* (llamada así porque la comunidad de los enrutadores ha convergido en una vista singular de topología). Una vista convergente en la topología significa que todos los enrutadores están de acuerdo sobre los vínculos que están funcionando, han dejado de funcionar, se ejecutan más rápido, etcétera.

Los protocolos de enrutamiento son la quinta esencia de las interconexiones de alta tecnología. Representan la capacidad de los dispositivos individuales, y aun de redes completas, para ayudar a administrarse. Se podría decir que las interconexiones se han vuelto orgánicas en el sentido de que los protocolos de enrutamiento son conscientes de sí mismos

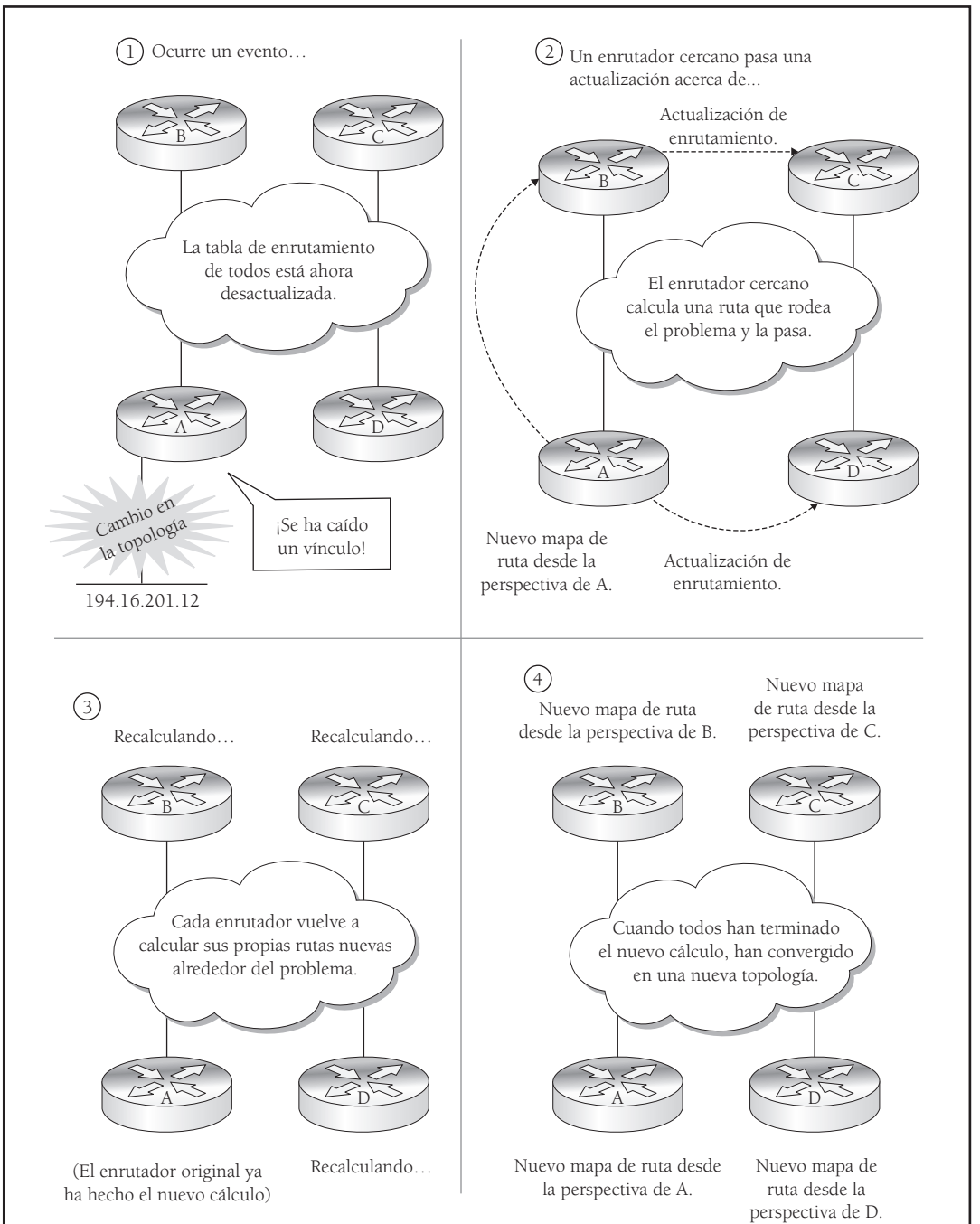


Figura 12-1. Los mensajes de actualización de enrutamiento coordinan las tablas de enrutamiento.

y se corrigen a sí mismos. A medida que las topologías crecen día a día o que las circunstancias cambian de un momento a otro, las interconexiones pueden responder, porque los protocolos de enrutamiento permiten a la comunidad de enrutadores conversar inteligentemente acerca de lo que deben hacer.

Un cliché de marketing sostiene que "la red es el sistema". Si eso fuera verdad, entonces los protocolos de enrutamiento servirían como el sistema operativo de la red. Los límites de los protocolos de enrutamiento están fijados en términos prácticos por el tamaño de la interconexión y su complejidad. No es exageración establecer que el desarrollo de protocolos de enrutamiento sofisticados es lo que ha hecho posible el crecimiento explosivo de Internet.

NOTA El Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco), el Hot Standard Routing Protocol (HSRP, protocolo activo de enrutamiento en espera) y otros protocolos especializados también se denominan a veces como protocolos de enrutamiento. Para nuestros objetivos, un protocolo de enrutamiento es el que coordina el intercambio de actualizaciones de enrutamiento para notificar a otros enrutadores los cambios de topología y aplicar un algoritmo para volver a calcular las rutas óptimas a través de una interconexión.

Comparación entre redes enrutadas y redes conmutadas

Una buena manera de explicar los protocolos de enrutamiento es la comparación. ¿Recuerda las tablas de conmutación del capítulo 5. Para recordarlo: los conmutadores llevan registro de las topologías de red conmutada por la fuerza bruta. Cada vez que llega un mensaje, el conmutador asocia la dirección MAC del origen del marco (dirección física de la capa dos) con el puerto conmutado del que proviene y hace una entrada en su tabla de direcciones MAC. De esta manera, el conmutador construye una lista de direcciones MAC de destino para cada puerto conmutado. He aquí el diseño básico de una tabla de direcciones conmutadas:

Direcciones MAC de destino	Puerto conmutado de destino
0060.2fa3.fabc	Fast Ethernet0/8
0050.0465.395c	Fast Ethernet0/4
0010.5a9b.b5e6	Fast Ethernet0/12
⋮	⋮

Ésta no es una manera particularmente inteligente de elaborar mapas de rutas, porque la tabla de direcciones MAC del conmutador sólo ve el siguiente paso. La tabla no dice nada acerca de la ruta completa al destino; simplemente le muestra la puerta siguiente. La manera en que un conmutador puede reducir el número de saltos que un marco debe tomar entre conmutadores es compilar tablas de dirección MAC cada vez más grandes y más grandes, incrementando por tanto las posibilidades de que se encuentre la mejor ruta. Los diseñadores de los conmutadores llaman a esto "optimización", pero lo que realmente se está optimizando son las direcciones MAC. (En caso de que se esté preguntando como eligen los conmutadores entre rutas alternas, éstos favorecen las rutas que se usan con más frecuencia, que son las que aparecen al principio de la lista de direcciones MAC.)

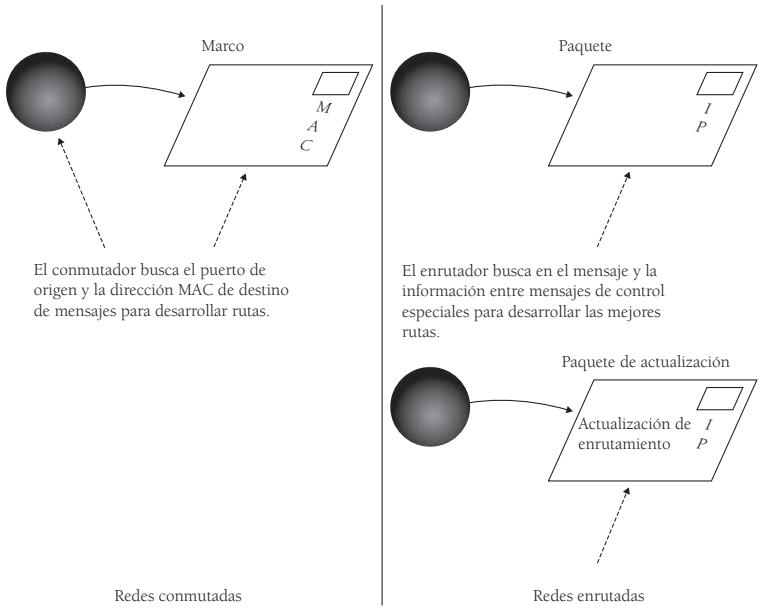


Figura 12-2. Los enrutadores usan mensajes de control para actualizar las tablas de enrutamiento, los conmutadores no.

Los enrutadores, en contraste, *pueden* ver más de un paso adelante. Las tablas de enrutamiento le dan a los enrutadores la capacidad de ver más allá en la interconexión sin ampliar su lista. Donde sustituyen los conmutadores la cantidad por la calidad, los enrutadores aplican la inteligencia. He aquí el diseño básico de un tipo simple de tabla de enrutamiento:

Destino	Siguiente salto	Cuenta de saltos
209.98.134.126	209.126.4.38	3
	127.197.83.128	5
	202.8.79.250	9
.	.	.
.	.	.
.	.	.

Este ejemplo tal vez no parezca demasiado, pero es "más inteligente" que la tabla de conmutación en una manera fundamental. El conmutador juega a las apuestas, pero el enrutador juega de manera inteligente, porque la columna cuenta de saltos le da al enrutador información adicional acerca de toda la ruta. Al saber cuántos enrutadores debe saltar un paquete para alcanzar su destino ayuda al enrutador que envía a elegir la mejor ruta. Este tipo de medida es denominada *medición de enrutamiento*, o *medición* simplemente para abreviar. Las mediciones como la cuenta de saltos son lo que separa al enrutamiento del método abrupto de "fuera de esta puerta, por favor" del conmutador. Las mediciones proporcionan

la inteligencia necesaria para los algoritmos de enrutamiento para calcular las mejores rutas a través de las interconexiones.

Las actualizaciones de enrutamiento son mensajes de control

Las redes enrutadas transportan un flujo subterráneo de tráfico especializado que intercambia mensajes de actualización de enrutamiento. Las redes conmutadas no hacen esto; adivinan lo que está pasando al mirar sólo las direcciones MAC de origen y el puerto entrante de paquetes de carga. Un *mensaje de carga útil*, por cierto, es el que lleva contenido útil de una aplicación en lugar de las operaciones internas de la interconexión. En la figura 12-2 se presenta un esquema de la diferencia.

Las actualizaciones de enrutamiento no son mensajes de carga útil, son *mensajes de control*. El contenido que entregan es usado por la interconexión para operaciones internas. Este segundo tipo de tráfico transporta actualizaciones de enrutamiento es la sangre de la interconexión, que entrega la inteligencia de una interconexión de tener que actuar de una manera unitaria y sobrevivir ante el cambio. Dada su importancia, para alcanzar una comprensión básica de los protocolos de enrutamiento, necesita saber lo que contienen las actualizaciones de enrutamiento, cuándo y dónde se enviaron y cómo son procesadas.

Enrutamiento dinámico en comparación con estático

Antes de seguir más adelante, viene al acaso un poco de antecedentes. Existen dos tipos básicos de enrutamiento:

- ▼ **Enrutamiento estático** Una ruta estática es una ruta fija preprogramada por un administrador de red. Las rutas estáticas no pueden utilizar los protocolos de enrutamiento y no se actualizan a sí mismas después de recibir mensajes de actualización de enrutamiento; deben actualizarse manualmente.
- ▲ **Enrutamiento dinámico** Este tipo se hace posible al enrutar protocolos, que calculan automáticamente las rutas con base en la actualización de enrutamiento. Casi todas las rutas de interconexión son dinámicas.

Esta distinción se hace aquí para llegar a un punto clave. No todas las rutas se calculan automáticamente (dinámicamente) mediante protocolos de enrutamiento, y por una buena razón. En casi todas las situaciones, los administradores de red optaran por retener el control directo sobre una minoría de rutas.

El mejor ejemplo de la manera en que las rutas estáticas se usan es la gateway predeterminada. Un enrutador no puede saber todas las rutas a todos los destinos, de modo que es configurado con una ruta de *gateway predeterminada* a la que los paquetes con destinos desconocidos se envían. Las gateways predeterminadas se ingresan como rutas estáticas para asegurarse que el tráfico no enviado se dirige a un enrutador que tiene entradas de tablas de enrutamiento que llevan fuera de la interconexión. En la figura 12-3 se muestra una gateway predeterminada en acción en dos lugares: primero en la PC, que se ha indicado que su gateway predeterminada es una interfaz de un enrutador particular; luego en el enrutador, donde su gateway predeterminada está fuera de su interfaz de Internet.

La capacidad de los protocolos de enrutamiento para la selección automática de la tabla de enrutamiento es algo bueno, pero sólo en una dosis pequeña. El uso de las rutas estáticas como gateway predeterminadas para manejar mensajes no anticipados ejemplifica esto.

Los enrutadores colaboran para obtener la convergencia

La convergencia es cuando todos los enrutador desde una interconexión están de acuerdo en una topología común. Por ejemplo, si un vínculo de red particular se ha caído, la interconexión habrá convergido cuando todos los enrutadores coinciden en nuevas rutas que ya no incluyen ese vínculo. Sin embargo, el enrutador debe tener sus propias rutas que se encuentran en su posición única en la topología de red. Por tanto, los enrutadores actúan de manera colectiva al compartir actualizaciones, pero aun toman acciones independientes al calcular sus propias rutas. Cuando el proceso está completo, han convergido, en el sentido de que todas las rutas se calcularon con base en un conjunto común de suposiciones acerca de las topologías actuales de la red.

Esta colaboración se orquesta mediante el protocolo de enrutamiento de la interconexión. Al hacer que las rutas funcionen de manera colectiva le da a las interconexiones su fortaleza, porque pueden tomar más de una ruta para aislar un problema en la red. Y, hasta que el problema es aislado, ningún enrutador tiene la información necesaria para calcular nuevas rutas alrededor del problema.

Cómo perciben los enrutadores los cambios en la topología

Los enrutadores usan protocolos de descubrimiento de gateway para llevar registro de los demás. Un *protocolo de enrutamiento de gateway* es un sistema que coordina el intercambio de

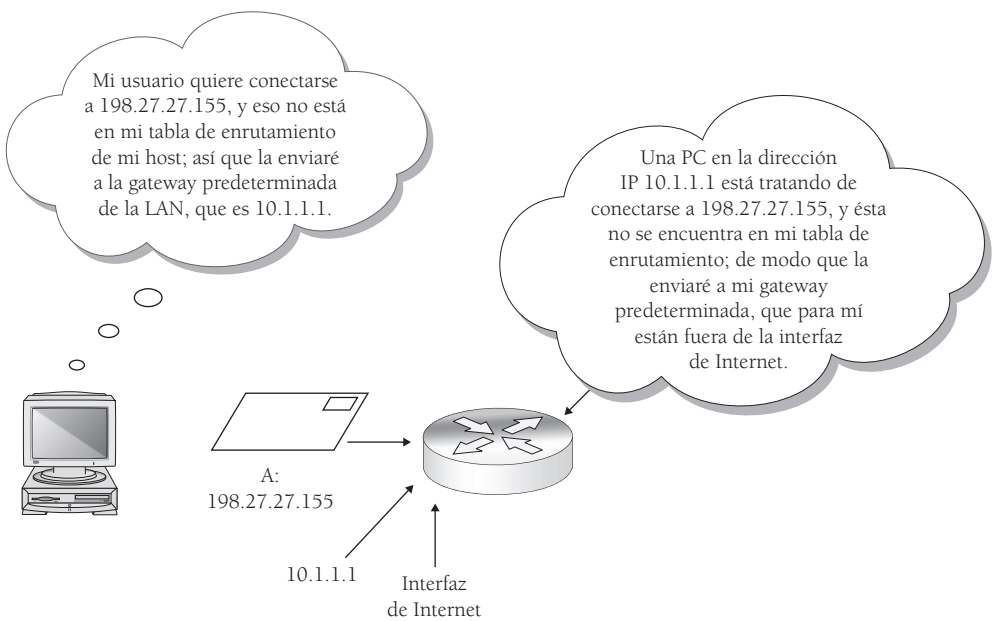


Figura 12-3. En el ejemplo clásico de una ruta estática es la gateway predeterminada de una red.

pequeños mensajes "¿todavía estás allí?" entre enrutadores en una interconexión, principalmente como una manera de percibir los vínculos caídos:

- ▼ Cada enrutador transmite mensajes "Hola" a sus enrutadores vecinos inmediatos en el intervalo fijado (digamos, una vez cada 90 segundos).
- ■ Si no se recibe un ACK (Acknowkledgment message, mensaje de reconocimiento) dentro de un periodo específico (tres minutos), la ruta se declara no válida.
- ▲ Si no se ha regresado un ACK en un periodo más largo (siete minutos), el enrutador y sus rutas se eliminan de la tabla del enrutador que envía, y se emite una actualización de enrutamiento acerca de todas las rutas que incorporan el enrutador que no responde como un vínculo.

Los protocolos de descubrimiento de gateway son protocolos de control de baja sobrecarga que las redes IP están enviando con el uso del protocolo de transporte UDP. En la figura 12-4 se ilustra la manera en que funciona.

Además de los problemas de percepción, los protocolos de descubrimiento de gateway detectan el aspecto del nuevo equipo. Los cuatro tipos de mensajes de descubrimiento de gateway de la figura 12-4 se denominan de manera colectiva como *cronómetros*.

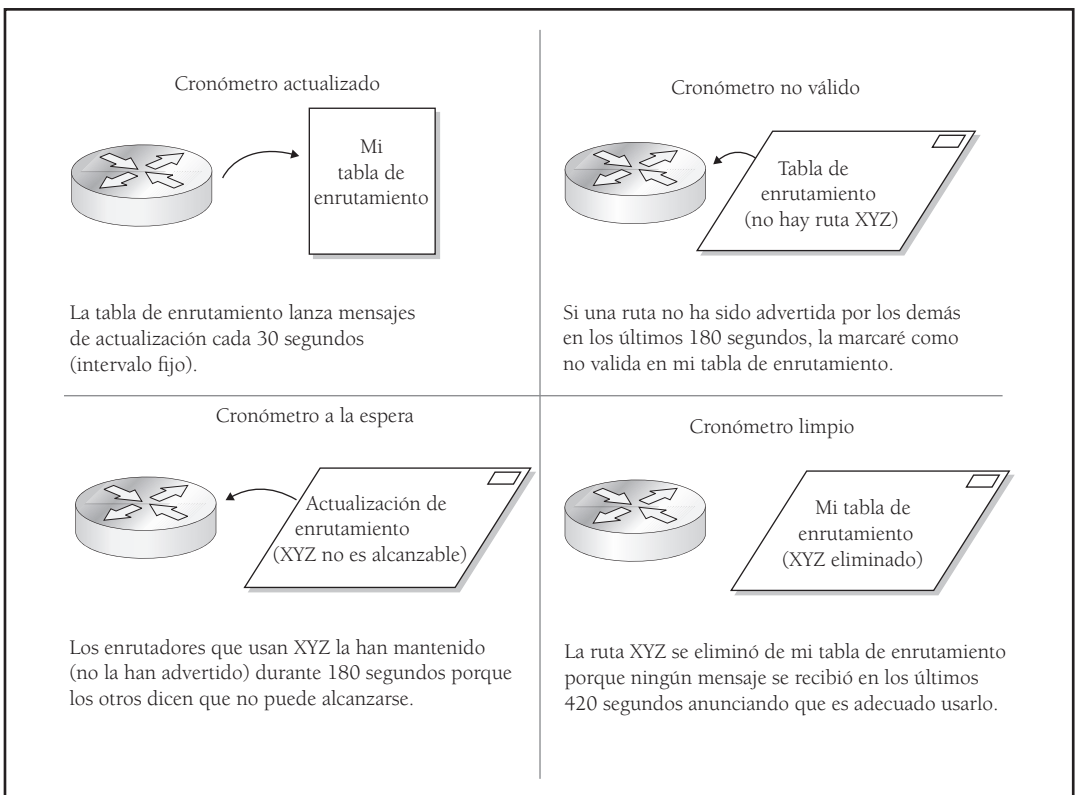


Figura 12-4. Los protocolos de descubrimiento de gateway usan cronómetros para detectar los cambios en la topología.

Cómo convergen las actualizaciones de enrutamiento

La percepción de un cambio en la topología es sólo el primer paso. A partir del punto del descubrimiento, las actualizaciones de enrutamiento deben pasarse hasta que todos los educadores puedan converger en una nueva topología al incorporar los cambios.

Tomemos un ejemplo. En la figura 12-5 se muestra una topología relativamente simple de cuatro enrutadores con redundancia de rutas, en que los mensajes tienen rutas alternas a los destinos. Un mensaje enviado de producción a contabilidad podría viajar a través del enrutador de investigación y desarrollo o de mercadotecnia. Si los paquetes que se envían de producción a través del enrutador de investigación y desarrollo al servidor de recorte de gastos de pronto ya no puede enviarse, no puede defenderse del enrutador de contabilidad para diagnosticar el problema por cuenta propia. Esto se debe a que hay demasiadas fuentes

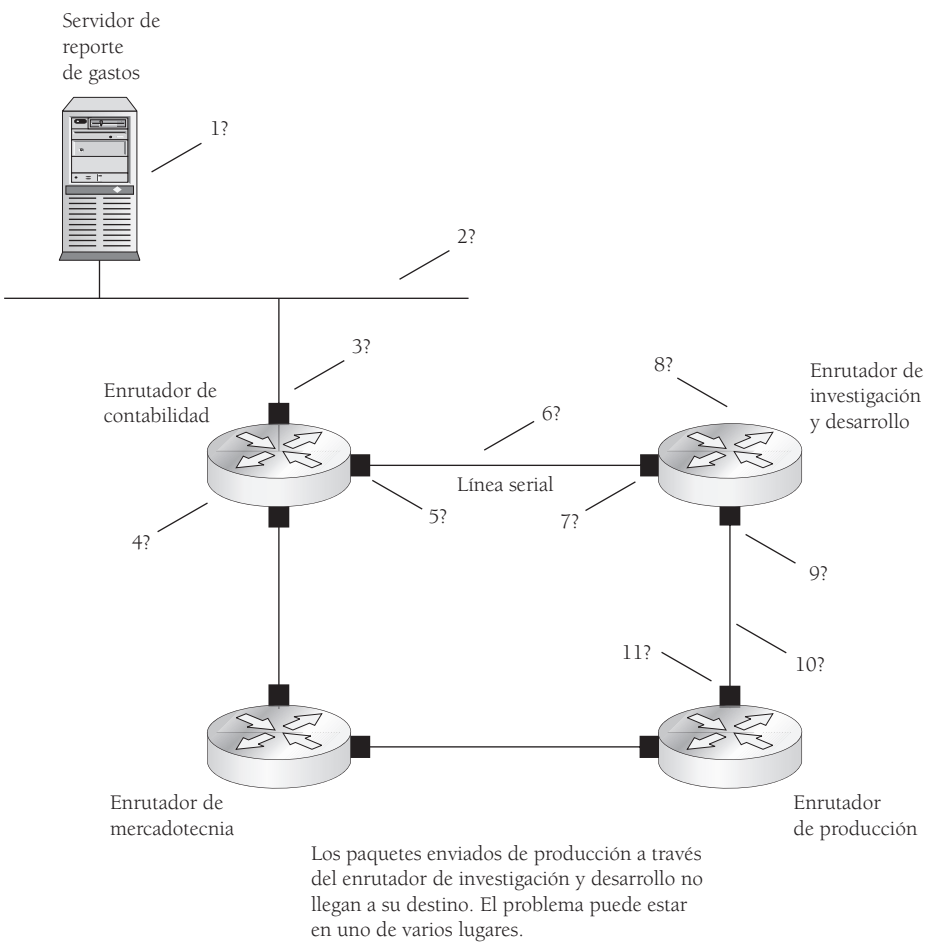


Figura 12-5. Los enrutador deben colaborar para localizar los problemas en la red.

posibles del problema, como se describe en las marcas de interrogación en la figura 12-5. He aquí un resumen de los hechos más probables que estarían causando el problema:

1. El servidor de reporte de gastos ha dejado de funcionar.
2. La conexión LAN al servidor de reporte de gastos ha fallado.
3. La interfaz del enrutador de contabilidad al segmento LAN del servidor de reporte de gastos ha fallado.
4. El enrutador de contabilidad ha fallado por completo.
5. La interfaz serial del enrutador de contabilidad al enrutador de investigación y desarrollo ha fallado.
6. La línea de transmisión serial que conecta a contabilidad con investigación y desarrollo ha dejado de funcionar.
7. La interfaz serial de investigación y desarrollo al enrutador de contabilidad ha fallado.
8. El enrutador de investigación y desarrollo ha fallado por completo.
9. La interfaz serial de investigación y desarrollo al enrutador de producción ha fallado.
10. La línea de transmisión serial que conecta a investigación y desarrollo con producción ha dejado de funcionar.
11. La interfaz serial de producción al enrutador de investigación y desarrollo ha fallado.

El enrutador de contabilidad no puede tener un conocimiento definitivo de los problemas uno, siete u ocho, porque no es responsable directo de sus dispositivos de red, y el enrutador de contabilidad no tendría ningún uso en caso de que pasara lo indicado en el problema cuatro.

Los paquetes no pueden encontrarse para dar un rodeo a la falla hasta que el problema sea localizado. Además, el problema debe localizarse para que los enrutadores converjan en una nueva topología de red (después de la falla).

Y aparte si, en nuestra topología de ejemplo, la línea serial entre contabilidad e investigación y desarrollo ha fallado, ambos enrutadores percibían esto al mismo tiempo y actualizan el problema. En la figura 12-6 se da seguimiento a la actualización de enrutamiento a medida que fluye de los enrutadores de contabilidad e investigación y desarrollo. Una vez que el enrutador ha percibido el problema, elimina la ruta fallida de su tabla de enrutamiento. Esto a su vez hace que el algoritmo de enrutamiento calcule una mejor ruta nueva a todos los destinos que han incorporado el vínculo con falla. Cuando estas nuevas rutas se calculan, el enrutador los emite en un mensaje de actualización de enrutamiento enviado a los demás enrutadores de la interconexión.

La información de enrutamiento actualizada se envía de los enrutadores de contabilidad e investigación y desarrollo para anunciar que ya no están usando la línea serial de sus rutas. Estos son mensajes de actualización de enrutamiento. Los enrutadores de producción y mercadotecnia, a su vez, reemplazan cualquier ruta que esté usando el vínculo serial. En el ejemplo de la figura 12-6, se toman dos actualizaciones de enrutamiento para la interconexión para converger en una nueva topología que deje a un lado la línea serial. Cuando esta se regresa otra vez al funcionamiento, los anotadores conectados también percibirán el cambio en la topología, y todo el proceso de actualización de rutas se repetirá a la inversa.

El tiempo de convergencia corto es un objetivo principal del diseño cuando se distribuye la topología de una interconexión. En redes grandes, puede tardar varias actualizaciones

para converger. La longitud del tiempo de convergencia depende del protocolo de enrutamiento usado, el tamaño de la interconexión y en qué lugar de la topología ha tenido lugar un cambio. Por ejemplo, si el problema de la figura 12-5 ha ocurrido tras la gateway del enrutador de contabilidad, sólo éste habría originado una actualización de enrutamiento, que habría dado como resultado un tiempo de convergencia de tres actualizaciones.

Los tiempos de convergencia largos son un síntoma de una interconexión que funciona mal. Muchos factores pueden hacer más lenta la convergencia, pero el principal es la demora en la propagación.

Demora de propagación

Un fenómeno que ocurre en las redes llamado *demora en la propagación* es el retraso entre el momento en que se envía un paquete y el momento en que llega su destino. La de la preparación no es un asunto simple de distancia geográfica o de conteo de saltos; también pueden influir otros factores. En la figura 12-7 se muestran varios factores de demora en la propagación.

Resulta obvio que algo tan básico como el tiempo requerido para que los datos viajen en la red es importante a todas las áreas de la interconexión. Pero la demora de propagación es un factor para lograr protocolos de enrutamiento, porque no todos los enrutadores reciben una actualización de enrutamiento al mismo tiempo. No importa la rapidez del medio de la red, la convergencia toma tiempo, a medida que una actualización de enrutamiento se pasa de un enrutador a otro hasta que llega al enrutador más lejano.

La importancia de la demora de la propagación crece con el tamaño de la interconexión. Las interconexiones grandes tienen docenas de enrutadores y cientos de segmentos LAN conectados (cada uno es una fuente posible de cambios en la topología). Siendo todo lo demás igual, cuanto más grande sea la red, mayor será su demora de propagación; y cuantas más rutas redundantes se usen, mayor será la posibilidad de confusión.

Bucles de enrutamiento

La demora en la propagación no plantearía un problema a los protocolos de enrutamiento si los enrutadores siempre condicionan antes que cualquier nuevo cambio surgiera. Pero no lo hacen. Cuanto más largas sean las demoras en la propagación de una interconexión, más susceptibles serán, algo denominado bucle de enrutamiento. Un *bucle de enrutamiento* es cuando los paquetes de carga útil no pueden alcanzar su destino debido a que la información de la tabla de enrutamiento está en conflicto. Esto sucede en interconexiones grandes o en las que ocurren gran número de cambios, cuando un segundo cambio en la topología surge antes de que la red sea capaz de converger en el primer cambio.

Tomando el ejemplo mostrado en la figura 12-8, el enrutador de investigación y desarrollo percibe que la red 10.1.1.12 ha dejado de funcionar y emite una actualización de enrutamiento. Pero antes de que el enrutador de producción reciba la actualización, emite una actualización de enrutamiento que indica que la red 10.1.1.12 aún es adecuada (porque la actualización tiene rutas que incorporan esta red). Las actualizaciones de investigación y desarrollo y producción entran en conflicto y, dependiendo de la manera en que funcione el tiempo de espera, pueden confundir a los demás enrutadores e incluso pueden confundirse entre sí, lanzando a la interconexión en un bucle de enrutamiento.

Los bucles de enrutamiento también pueden perpetuarse a sí mismos. Si las actualizaciones de enrutamiento en conflicto son lo suficientemente persistentes, cada repetición anula a la otra en las decisiones de la ruta tomadas por los enrutadores afectados. Si la ruta

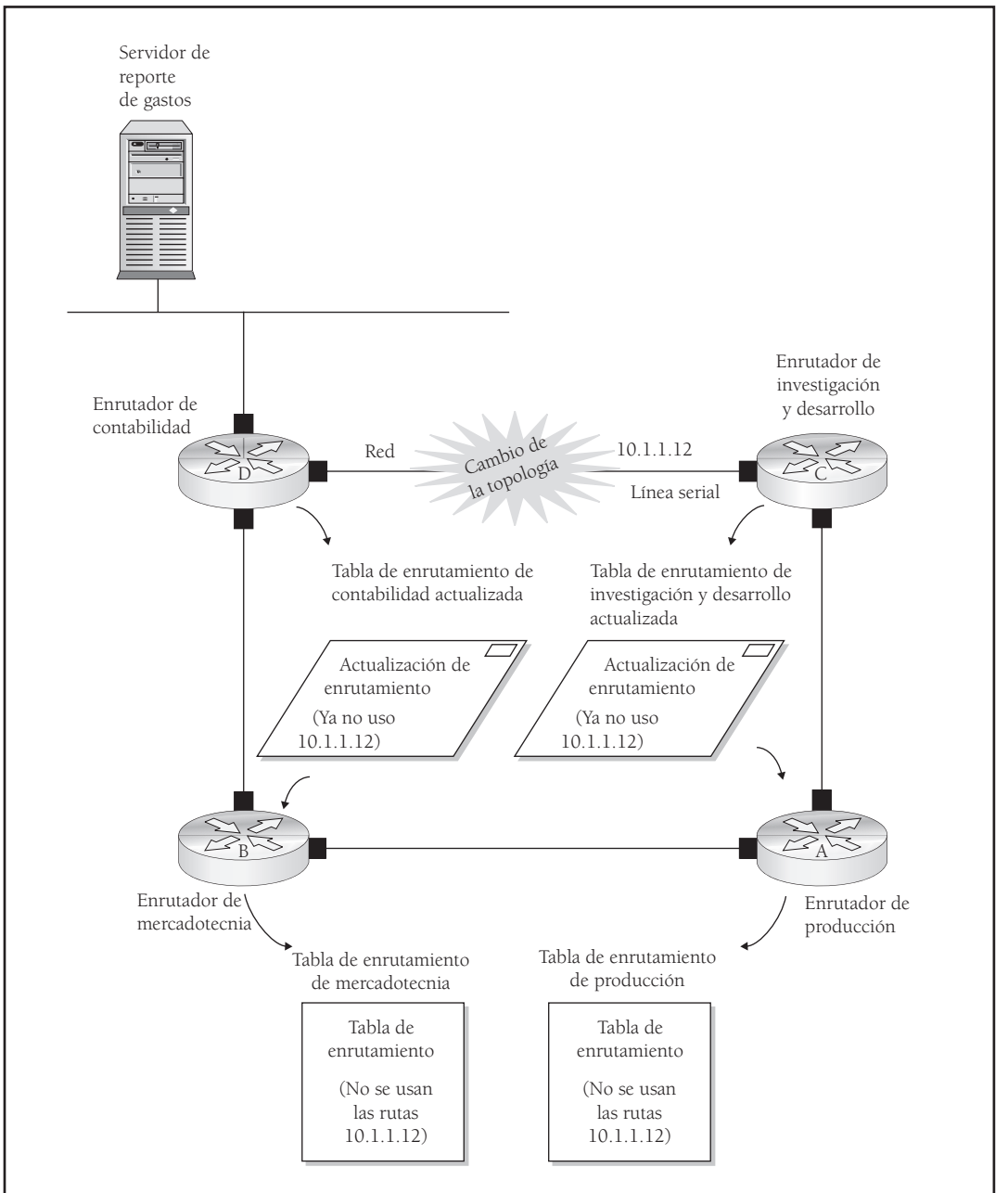


Figura 12-6. Sólo dos actualizaciones de enrutamiento son necesarias para la convergencia.

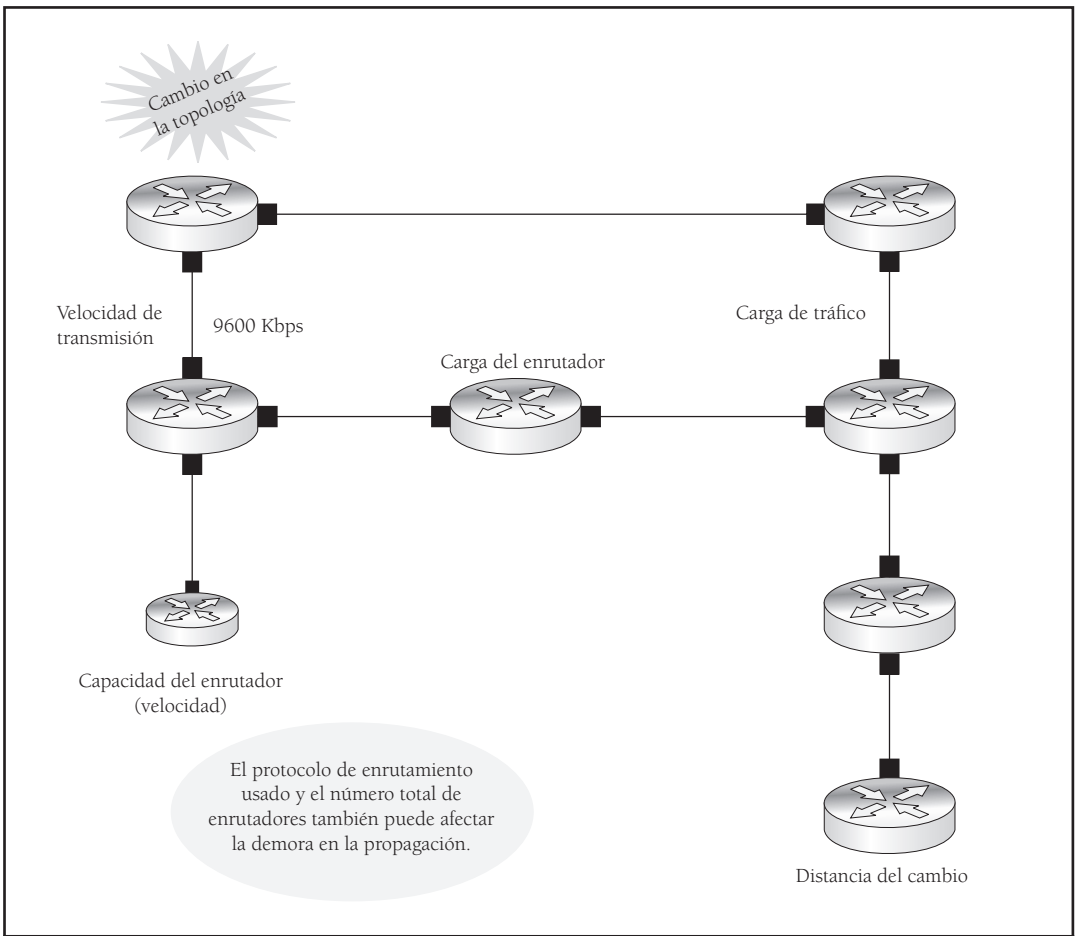


Figura 12-7. Varios factores pueden influir en la duración de la demora de propagación.

primaria del enrutador vacila cada vez que recibe una actualización, la interconexión se vuelve inestable, si las cosas se salen demasiado de balance (por ejemplo, hay demasiados bucles y las elecciones de ruta principales son volátiles), la topología colectiva del protocolo puede empezar a desintegrarse. La espiral descendente sigue este camino:

- ▼ Dos o más actualizaciones de enrutamiento en conflicto causan que los mensajes se enruten a través de rutas que no funcionan y, por tanto, no se entregan.
- ■ A medida que el buque persiste, se consume más ancho de banda debido a los paquetes de carga útil enrutados de manera ineficiente y las actualizaciones de enrutamiento tratan de corregir el problema.
- ▲ La reducción del ancho de banda desencadena aún más actualizaciones de enrutamiento como respuesta al empeoramiento de la velocidad de transmisión.

El círculo vicioso de un bucle de enrutamiento se describe en la figura 12-9.

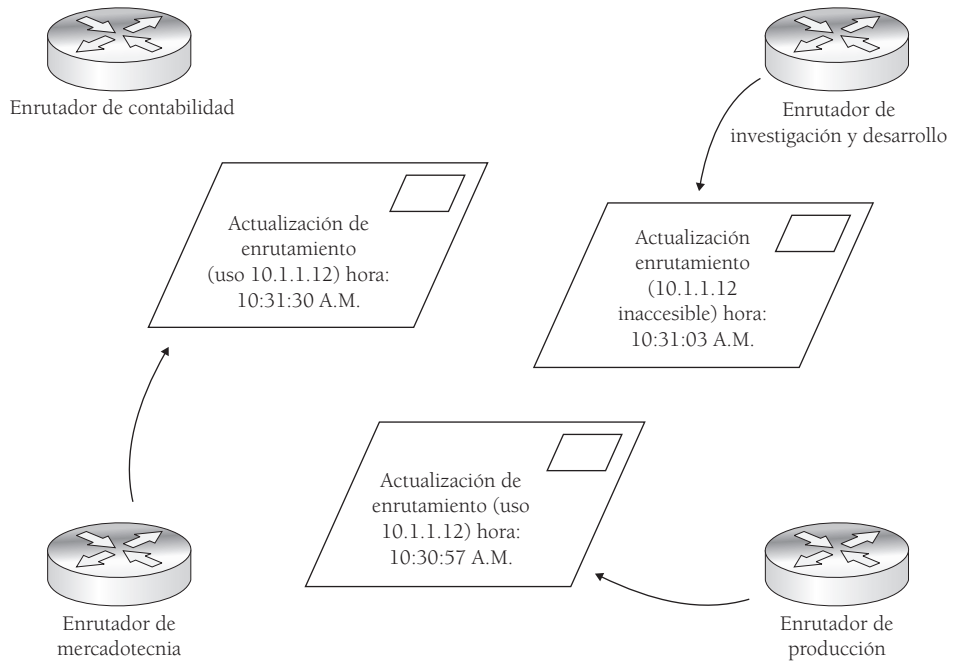


Figura 12-8. Un bucle de enrutamiento puede empezar cuando las actualizaciones de enrutamiento se superponen.

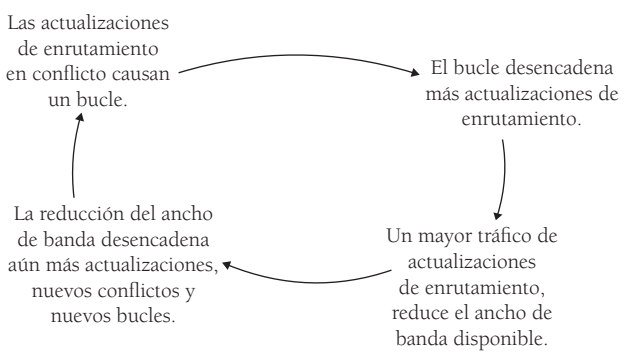


Figura 12-9. Si los eventos de la red desplazan a la convergencia, pueden ocurrir bucles infinitos.

Mecanismos para mantener a las interconexiones libres de bucles

Un escenario como el que se describió es inaceptable para operaciones de red efectivas. Los protocolos de enrutamiento incorporan varios mecanismos sofisticados para evitar el surgimiento de bucles de enrutamiento:

- ▼ **Cortes de transmisión** Supresión de anuncios acerca de una ruta que está en cuestionamiento el tiempo suficiente como para que todos los enrutadores conozcan su verdadero estado.
- ■ **Horizontes divididos** La práctica de no anunciar una ruta en la misma dirección de la propia ruta.
- ■ **Envenenamiento de actualizaciones inversas** Un mensaje de actualización de enrutamiento que explícitamente establece que una red o una subred no es alcanzable (en lugar de que un enrutador cercano simplemente la elimine de su tabla de enrutamiento por falta de uso).
- ▲ **Cuenta máxima de saltos** Los paquetes viajan un número máximo de saltos entre el origen y el destino. Una vez que han excedido su límite, son eliminados, lo que evita un bucle.

Cortes de transmisión Un *corte de transmisión* es una manera de ayudar a evitar que las malas rutas se restablezcan por error. Cuando una ruta se coloca en un estado de corte de transmisión, los anotadores no anunciarán la ruta ni aceptarán anuncios sobre ella por un intervalo específico llamado *periodo de corte de transmisión*. El corte de transmisión tiene el efecto de limpiar la información acerca de una mala ruta de las interconexiones. Es una manera impositiva de sacar una manzana podrida del barril para ayudar a reducir las oportunidades de que se inicie un bucle de enrutamiento. En el extremo, un periodo de corte de transmisión sería un intervalo ligeramente más largo de lo que normalmente toma toda la red en conocer un cambio en el enrutamiento (su tiempo de convergencia promedio).

Pero detener la liberación de actualizaciones de enrutamiento obviamente hace más lenta la convergencia, de modo que hay que compensar duramente entre el beneficio aportado por prevención de bucles mediante los cortes de transmisión y la calidad del servicio de la red. Esto se debe porque al demorar la liberación de una actualización se deja en juego una mala ruta por un periodo más largo. En las interconexiones de cualquier tamaño, establecer

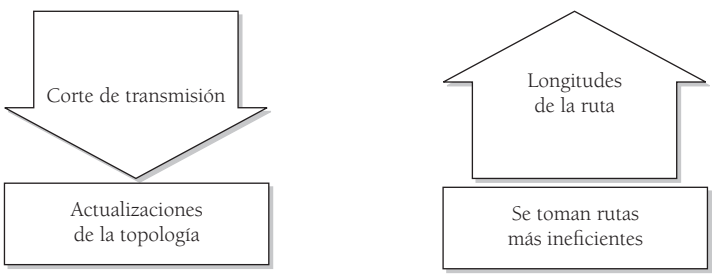


Figura 12-10. Los cortes de transmisión evitan los bucles de enrutamiento pero pueden hacer más lento el rendimiento de la red.

intervalos de corte de transmisión para que coincidan con la convergencia promedio da como resultado mensajes frecuentes de tiempo de espera para el usuario final. En la realidad, los tiempos de corte de transmisión suelen establecerse en un intervalo mucho menor que el tiempo de convergencia promedio de la red para aminorar parcialmente el riesgo de bucles, pero al mismo tiempo evitar un número mayor de avisos de tiempo de espera de la red para los usuarios. Este equilibrio se describe en la figura 12-10.

Horizontes divididos Un *horizonte dividido* es una configuración de enrutamiento que evita que una ruta se anuncie de regreso en la dirección de la que proviene. La teoría es que básicamente no tiene sentido enviar información de regreso a su origen. Un ejemplo de esto se esquematiza en la figura 12-11. El enrutador B, que se encuentra en medio, recibió una ruta a la red 10.1.99.0 del enrutador A, que se encuentra a la izquierda. La regla del horizonte dividido instruye al enrutador B a no incluir esa ruta en las actualizaciones que envía de regreso al enrutador A. La suposición es que el enrutador A era probablemente el origen de la ruta (dado que se encuentra en la dirección de la red 10.1.99.0) y, por tanto, no necesita ser informado acerca de la ruta. Si la interfaz del enrutador A hacia la red 10.1.99.0 deja de funcionar y no tiene la suficiente inteligencia integrada, tomaría su propia actualización de enrutamiento de regreso al enrutador B y trataría de usarla como una manera de rodear la interfaz que no funciona.

Los cortes de transmisión normalmente pueden evitar los bucles de enrutamiento por sí mismos, pero los horizontes divididos suelen configurarse como una medida de respaldo porque no hay una desventaja particular en el uso de ellos.

Envenenamiento de actualizaciones inversas Por ahora, tal vez haya notado que los protocolos de enrutamiento trabajan de manera implícita. En otras palabras, dirigen el tráfi-

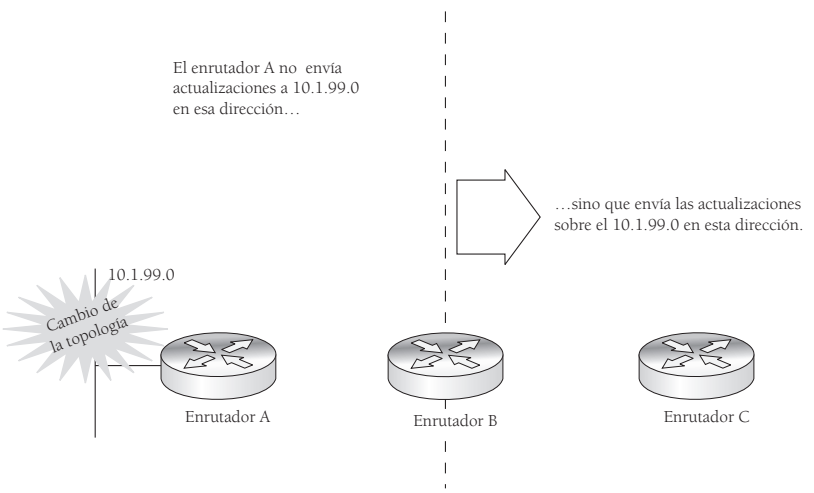


Figura 12-11. Un horizonte dividido evita que una actualización de enrutamiento haga eco de regreso a su origen.

co alrededor de un vínculo en mal estado al no incluir rutas que incluyan ese vínculo en las actualizaciones de enrutamiento. El *envenenamiento de actualizaciones inversas*, en contraste, establece de manera implícita que un vínculo es malo. El envenenamiento inverso funciona al hacer que el enrutador revise los aumentos excesivamente grandes en las mediciones. Las mediciones de enrutamiento están diseñadas de tal manera que un aumento refleja un deterioro. Por ejemplo, un aumento en el número de saltos que un enrutador tiene que tomar lleva a que sea menos deseable. Un enrutador compara una medición de actualización enrutamiento entrante para una ruta contra la que había cuando el propio enrutador había emitido una actualización anterior incluida la misma ruta. El protocolo de enrutamiento está configurado con un factor de aumento aceptable que, si se excede, hace que el enrutador suponga que la ruta es un mensaje "invertido". En la figura 12-12 se describe el proceso.

En los protocolos de enrutamiento de Cisco, el aumento predeterminado de una medición de enrutamiento es un factor de 1.1 o mayor. En otras palabras, si una ruta devuelve una actualización con una medición que es 110%, o mayor de lo que era cuando se envió hacia fuera, se supone que un bucle está en progreso. Por ejemplo, si un enrutador envía una actualización con una ruta con una medición de conteo de saltos de uno, y regresa en una actualización de otro enrutador con un conteo del saltos de dos, la suposición es que se encuentra dentro de un bucle. Cuando esto sucede, el enrutador se coloca en un estado de corte de transmisión en que ni envía ni recibe actualizaciones en esa ruta. El estado de corte de transmisión se mantiene por un periodo lo suficientemente largo como para limpiar el problema de un sistema de actualización (de allí su nombre de *envenenamiento inverso*). El bucle es una mala medición "invertida" en el enrutador; el corte de transmisión es una manera de "envenenar" (o matar) las actualizaciones que podrían contener una medición mala.

Los horizontes divididos son una buena manera de evitar los bucles del enrutamiento entre enrutadores adyacentes. Pero en las interconexiones grandes en que las actualizaciones de enrutamiento se pasan entre enrutadores muy lejanos entre sí, el envenenamiento de actualizaciones inversas ayuda a evitar que las malas rutas inicien bucles antes de que tenga lugar la convergencia de actualización.

Conteo máximo de saltos Esto alude al número de enrutadores que un paquete puede recorrer. Cada vez que un paquete se mueve hacia un enrutador, se agrega otro salto a la cuenta. Una vez que alcanza el número dado de saltos, el paquete se descarta.

Los conteos de saltos se usan para evitar problemas causados por bucles. Por ejemplo, si el número máximo de saltos es de 15, entonces si el paquete recorre 14 enrutadores, si en el siguiente salto no llega a su destino, será eliminado. Esto evita que los paquetes salten eternamente de un enrutador al siguiente.

Mediciones de enrutamiento

Una medición de enrutamiento es un valor usado por un protocolo de enrutamiento para influir en las decisiones de enrutamiento. La información sobre mediciones se almacena en las tablas de enrutamiento y se usa en los algoritmos de enrutamiento para determinar las rutas óptimas a los destinos. Cuesta un poco de trabajo acostumbrarse a la terminología, pero he aquí las mediciones de uso más amplio:

- **Costo** No se trata de un costo financiero, sino de un número de "costo" teórico usado para representar el tiempo, la dificultad, el riesgo y otros factores relacionados con una ruta.

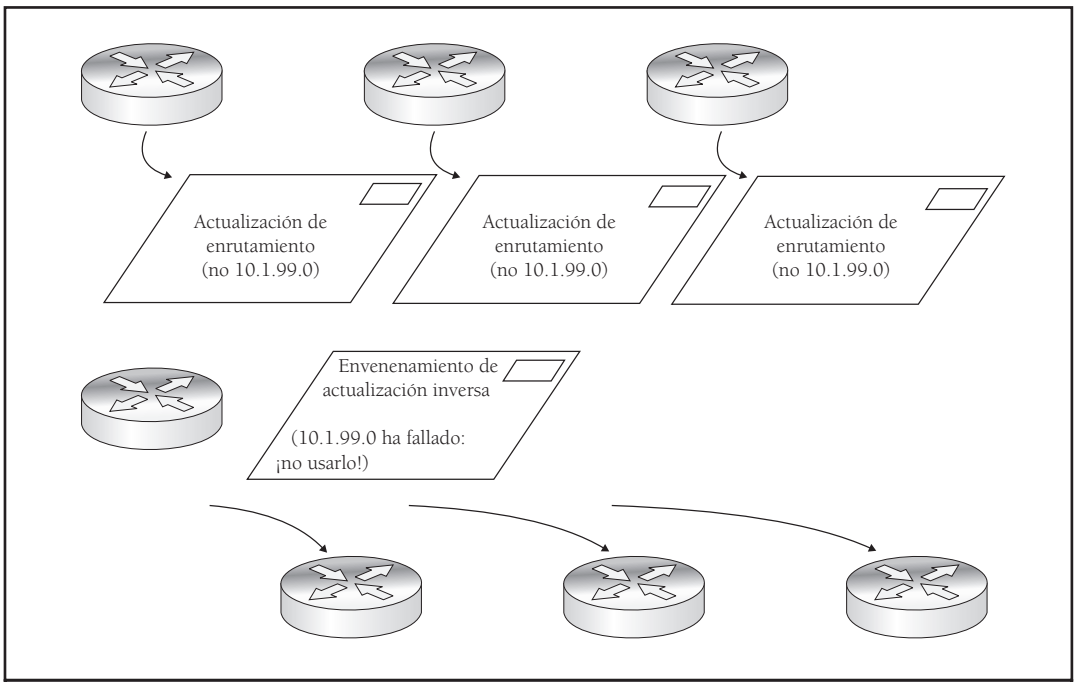


Figura 12-12. La mayor parte de las actualizaciones de enrutamiento son correcciones implícitas; el envenenamiento de actualizaciones inversas es explícito.

- **Distancia** No se trata de la distancia física en millas o de los metros de cable, sino de un número de "distancia" teórica. La mayor parte de las mediciones de distancia se basan en el número de saltos de una ruta.
- **Ancho de banda** El ancho de banda de un vínculo de red (100 Mbps, por ejemplo).
- **Carga de tráfico** Número que representa del tráfico (como el número y tamaño de paquetes) que viaja por un vínculo durante un periodo específico.
- **Demora** En este contexto, el tiempo entre el inicio de un ciclo de actualización de enrutamiento y cuando todos los enrutadores de una interconexión convergen en una sola vista de topología (también llamada *demora de propagación* o *latencia*).
- **Confiabilidad** Número relativo usado para indicar la confiabilidad de un vínculo.
- **MTU** El tamaño máximo de paquetes (Maximum Transmission Units) que una interfaz de red particular puede manejar, por lo general expresada en bytes.

NOTA En ocasiones "costo" se usa como un término general para el resultado calculado por una ecuación dentro del algoritmo de protocolo de enrutamiento. Por ejemplo, alguien podría establecer que el costo general de una ruta era más que la de otra, cuando en realidad el algoritmo de enrutamiento usó mediciones para distancia, ancho de banda, carga de tráfico y demora.

Algunos protocolos de enrutamiento simples usan sólo una medición. Sin embargo, por lo general más de una medición de enrutamiento se utiliza para determinar las rutas

óptimas. Por ejemplo, una ruta de dos saltos que viaja por una línea serial de 9 600 Kbps va a ser mucho más lenta que una ruta de tres saltos que va por un circuito T3 a 44 Mbps. No es necesario ser Euclides para imaginarse que mover un bit 4 000 veces más rápido compensa en exceso el salto adicional.

Los protocolos de enrutamiento sofisticados no sólo soportan varias mediciones, también le permiten decidir cuál usar. Además, puede asignar pesos relativos a las mediciones e influir de manera más precisa en la selección de la ruta. Si el administrador de la red establece apropiadamente las mediciones, el comportamiento general de la interconexión puede afinarse mejor para los objetivos de la empresa. En la figura 12-13 se muestran algunas mediciones de enrutamiento en acción. Y aparte todos los protocolos de enrutamiento de Cisco vienen con una configuración predeterminada para estas mediciones. Estas configuraciones predeterminadas se basan en cálculos de diseño hechos en los laboratorios de Cisco y a partir de la experiencia real obtenida en el campo. Si alguna vez mete sus manos en un protocolo de enrutamiento, piénselo mucho antes de que empiece a cambiar las configuraciones predeterminadas de medición. El efecto dominó de una mala decisión de medición de enrutamiento puede ser devastador. Las configuraciones de mediciones desequilibradas pueden manifestarse en la forma de un mal rendimiento de red y de bucles de enrutamiento.

Arquitecturas de protocolo de enrutamiento

Hay tres tipos básicos de arquitecturas de protocolo de enrutamiento:

- ▼ **Protocolos de enrutamiento distancia-vector** Algoritmos simples que calculan un valor de distancia acumulado entre enrutadores con base en la cuenta de saltos.
- ■ **Protocolos de enrutamiento vínculo-estado** Algoritmos sofisticados que mantienen una base de datos compleja de topología de interconexión.
- ▲ **Protocolos de enrutamiento híbridos** Combinación de métodos distancia-vector y vínculo-estado que tratan de incorporar las ventajas de ambos y minimizar sus desventajas.

Enrutamiento distancia-vector

Los primeros protocolos de enrutamiento distancia-vector usaban sólo una medición llamada distancia para calcular la mejor ruta a un destino. La distancia es el número de saltos de enrutador al destino. Los algoritmos distancia-vector (también llamados algoritmos de Bellman-Ford) operan un protocolo en que los enrutadores pasan actualizaciones de tabla de enrutamiento a sus vecinos inmediatos en todas las direcciones. A cada intercambio, el enrutador aumenta el valor de distancia recibido para una ruta, con lo que aplica su propio valor de distancia a ella. La tabla de actualización se pasa entonces más hacia fuera, donde los enrutadores receptores repiten el proceso. La teoría fundamental es que no es necesario que cada enrutador sepa todo acerca de los demás vínculos, sólo que están allí y cuál es la distancia aproximada a ellos. En la figura 12-14 se describe el proceso de actualización enrutamiento distancia-vector.

El enrutamiento distancia-vector puede tener una convergencia lenta. Esto se debe a que las actualizaciones de enrutamiento se disparan mediante cronómetros para que tengan lugar en intervalos predeterminados, no como respuesta a un evento en la red que causa un cambio en la topología. Esto hace que resulte más difícil para los protocolos distancia-vector responder rápidamente al estado de una condición operativa de un vínculo actual.

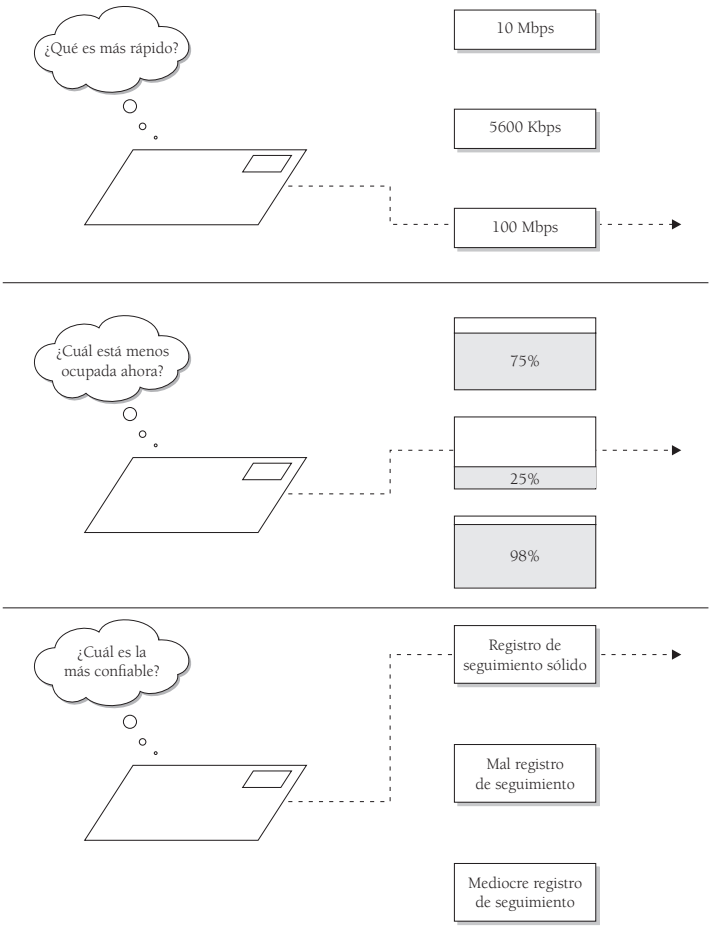


Figura 12-13. Las mediciones de enrutamiento se usan para influir en las decisiones que toman los algoritmos de enrutamiento.

Si un vínculo de red deja de funcionar, el sistema distancia-vector debe esperar hasta que el siguiente ciclo de actualización programado pase el vínculo que dejó de funcionar para recogerlo y pasar una tabla de enrutamiento actualizada (menos el vínculo que dejó de funcionar) a través de la interconexión.

NOTA El nombre "distancia-vector" puede resultar confuso, porque algunos protocolos avanzados distancia-vector usan mediciones de enrutamiento diferentes de la distancia teórica. En realidad, algunas instalaciones llamadas distancia-vector sólo dependen parcialmente de la medición de la cuenta de saltos. La mejor manera de considerar los protocolos distancia-vector, es que actualizan las topologías de enrutamiento a intervalos fijos.

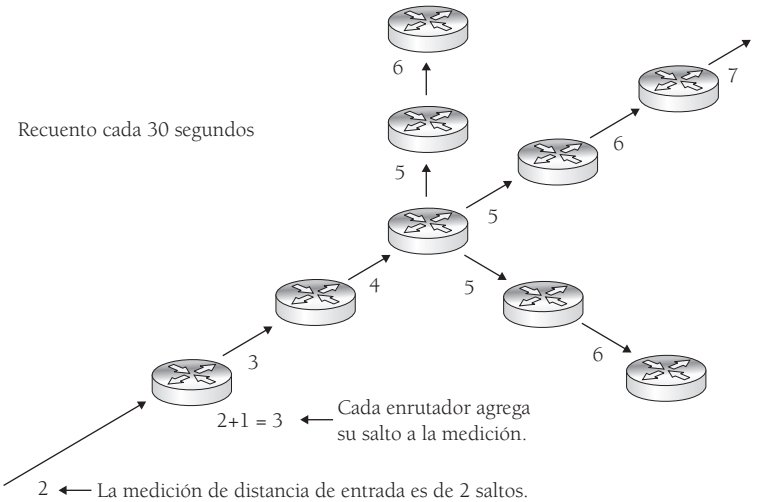


Figura 12-14. El enrutamiento distancia-vector propaga las actualizaciones de enrutamiento a intervalos fijos.

Depender de actualizaciones a intervalos fijos hace que los protocolos distancia-vector sean más lentos en la convergencia sobre los cambios de la topología y, por tanto, más susceptibles a los bucles de enrutamiento. Además, la mayor parte de los protocolos distancia-vector están limitados a 16 saltos y por lo general se usan en interconexiones con menos de 50 enrutadores.

A pesar de sus maneras poco sofisticadas, los protocolos distancia-vector son, por mucho, los de uso más amplio. Aunque el método es simple y fácil de configurar, no se escala bien. Por otra parte, debido a que no hace una gran cantidad de cálculos, consume poco CPU del enrutador o recursos de memoria. Por lo general, los algoritmos distancia-vector son lo suficientemente buenos para adaptarse a los cambios de la topología encontrados en interconexiones más pequeñas. Los protocolos de enrutamiento distancia-vector que se instalan más ampliamente son RIP e IGRP.

Enrutamiento vínculo-estado

El enrutamiento vínculo-estado está orientado a eventos. También conocido como *shortest path first* (*SPF*, *primero el vínculo más corto*), estos protocolos se concentran en el estado de los vínculos de interconexión que forman las rutas. Cada vez que cambia el estado de un vínculo, una actualización de enrutamiento llamada *link-state advertisement* (*LSA*, *anuncio vínculo-estado*) se intercambia entre enrutadores. Cuando un enrutador recibe una actualización de enrutamiento LSA, el algoritmo vínculo-estado se usa para volver a calcular la ruta más corta a los destinos afectados. El enrutamiento vínculo-estado trata de mantener siempre un conocimiento completo de la topología de la interconexión al actualizarse asimismo de manera incremental cada vez que ocurre un cambio. En la figura 12-15 se describe el proceso vínculo-estado.

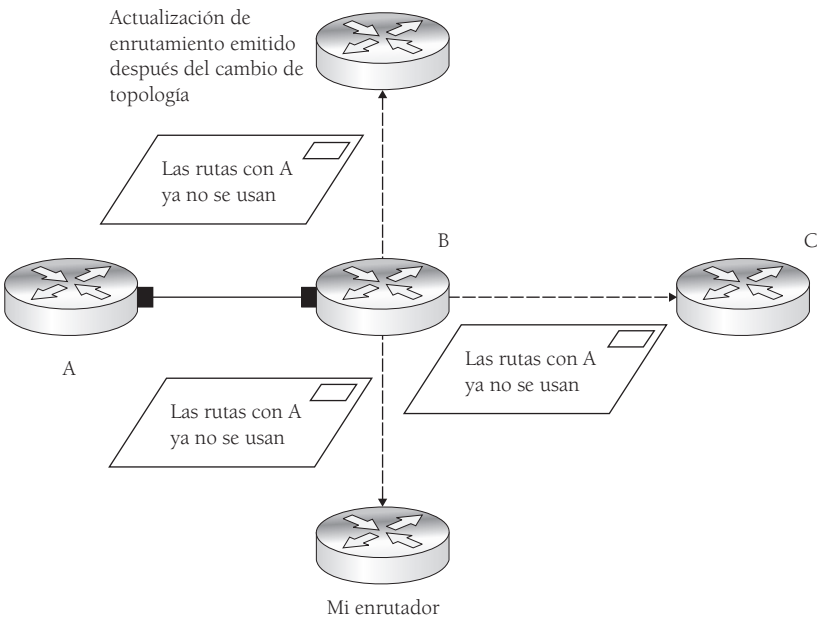
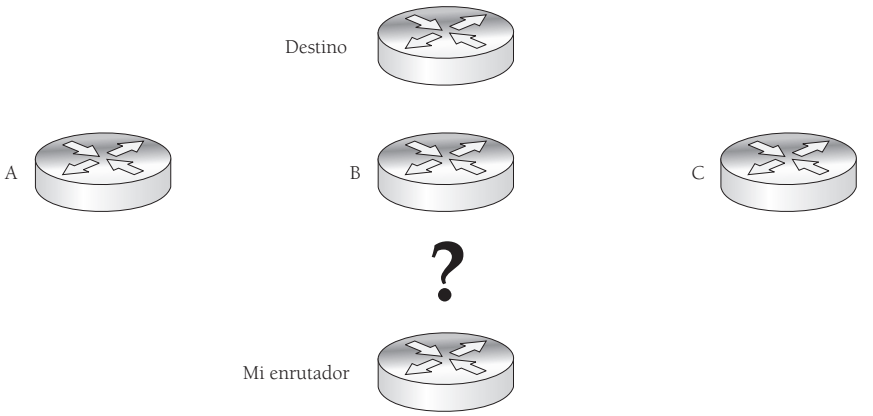


Figura 12-15. El enrutamiento vínculo-estado está orientado a eventos.

El algoritmo vínculo-estado hace mucho más que sólo hacer que un enrutador agregue su valor de distancia local a una distancia acumulativa. Después de que se recibe una actualización de LSA, cada enrutador usa el algoritmo para calcular un *árbol de ruta más corta* a todos los destinos. Los cálculos vínculo-estado se basan en el algoritmo de Dijkstra. Este proceso arroja rutas enteramente nuevas en lugar de simplemente aplicar nuevos valores de distancia a rutas preexistentes. Piense de esta manera: el enrutamiento distancia-vector coloca un nuevo valor en la misma ruta; el algoritmo SPF del enrutamiento vínculo-estado construye nuevas rutas completas pieza por pieza, desde el vínculo hacia arriba. SPF es capaz de hacer esto porque la base de datos vínculo-estado contiene información completa sobre los componentes de la interconexión y su topología.

Las rutas calculadas por SPF se ingresan en la tabla de enrutamiento actualizada. Estas entradas incluyen valores recalculados para todas las mediciones configuradas para uso en la implementación vínculo-estado. Posibles mediciones incluyen costo, demora, ancho de banda, confiabilidad y otras, con sus valores actualizados para reflejar la nueva ruta. Esto se hace al utilizar información de medición para cada vínculo incorporada en la ruta recién calculada. En la figura 12-16 se muestra la manera en que el algoritmo SPF elige la mejor ruta.

Hay otras dos ventajas en el enrutamiento vínculo-estado; ambas tienen que ver con la conservación del ancho de banda. Primero, debido a que las actualizaciones de LSA contienen sólo información acerca de las rutas afectadas, las actualizaciones de enrutamiento viajan más rápido y consumen menos ancho de banda. En segundo lugar, en el enrutamiento



Ruta	Estado	Costo (40%)	Distancia (10%)	Ancho de banda (20%)	Confiabilidad (30%)
Vía enrutador A	No funciona	100	5	100	75
Vía enrutador B	Funciona	50	5	100	75
Vía enrutador C	Funciona	100	4	1 000	100

Figura 12-16. El algoritmo SPF del enrutamiento vínculo-estado construye las rutas más cortas desde el vínculo hacia arriba.

distancia-vector, la mayor parte de los ciclos de actualización se desperdician porque tienen lugar aunque no haya un cambio de topología. Los ciclos de actualización innecesarios no sólo aumentan el excedente de uso del ancho de banda, sino que también incrementan las posibilidades de que actualizaciones de enrutamiento en conflicto converjan simultáneamente. Al emitir actualizaciones LSA cuando se requieran (además de sus intervalos de actualización regular) los protocolos vínculo-estado disminuyen la oportunidad de los conflictos que se perpetúan asimismo ocasionados por los bucles de enrutamiento.

Debido a que los protocolos vínculo-estado están orientados a eventos, no es necesario que la adaptación al cambio de topología esperen una serie de cronómetros preestablecidos para dispararse antes de que pueda empezar el proceso de convergencia. Esto no sólo hace que los protocolos vínculo-estado sean menos propensos a los bucles, sino que también los hace más poderosos porque ya no hay límite en el número de saltos en las rutas que calculan.

Las desventajas de los protocolos de enrutamiento vínculo-estado se relacionan principalmente con la logística y el costo. Durante las etapas iniciales de implementación, el tráfico LSA tiende a fluir en una interconexión con mensajes de control de construcción de bases de datos, haciendo cara la implementación. Debido a que realiza muchos cálculos, el enrutamiento vínculo-estado también puede utilizar considerablemente el enrutador del CPU y recursos de memoria del enrutador cuando es necesario hacer nuevos cálculos. Esto

significa que quienes consideran una actualización a un protocolo de enrutamiento vínculo-estado deben enfrentar la perspectiva de gastar dinero en actualizaciones de equipo. Sin embargo, tal vez la carga más pesada de los protocolos vínculo-estado es que son complicados. Se trata de protocolos de enrutamiento sofisticados que pueden resultar intimidantes para los administradores de redes, sobre todo quienes aún están aprendiendo. Los protocolos vínculo-estado mejor conocidos son OSPF e IS-IS.

Enrutamiento híbrido

Los protocolos de enrutamiento híbrido usan más mediciones distancia-vector exactas en un protocolo diseñado para converger de manera más rápida. Aunque los estándares abiertos se han desarrollado para el llamado enrutamiento hibridizado, el único producto de Cisco basado en el concepto es el Enhanced Interior Gateway Routing Protocol (EIGRP, protocolo de enrutamiento interior de gateway mejorados).

Cómo se implementan los protocolos de enrutamiento

De manera muy parecida a los firewall, los protocolos de enrutamiento toman su propia perspectiva particular del paisaje de la interconexión. Para un firewall, las redes están dentro o fuera, y las conexiones son controladas de acuerdo con ello. Los protocolos de enrutamiento tienen sus propias preocupaciones relacionadas con la recopilación y designación de topología actualizadas, no las conexiones. Por tanto, los protocolos de enrutamiento definen el paisaje de la red en términos de *interior* y *exterior*, donde un dominio de enrutamiento termina y otro empieza. Esto se debe a las necesidades de un enrutador de conocer cuáles otros enrutadores son parte de su propio dominio de enrutamiento (están en el interior) y, por tanto, deben compartir actualizaciones de enrutamiento.

Sistemas autónomos

El *control administrativo* se define como quien controla la configuración del equipo en una red. Debido a que Internet interconecta demasiadas entidades organizacionales, ha desarrollado el concepto de un sistema autónomo. Un sistema autónomo se define como una colección de redes que se encuentran bajo el control administrativo de una sola organización y que comparten una estrategia de enrutamiento común. Casi todos los sistemas autónomos son interconexiones operadas por corporaciones, los Internet Service Providers (ISP, proveedores de servicio de Internet), las agencias gubernamentales y las universidades.

Al revisar los tres sistemas autónomos de la figura 12-17, cada uno considera a las otras dos como sistemas autónomos exteriores (o externos). Esto se debe a que los otros dos se encuentran bajo el control administrativo de alguien más, y están ejecutando una estrategia de enrutamiento separada. Una estrategia de enrutamiento es un término usado para describir el hecho de que las actualizaciones de enrutamiento se están intercambiando bajo una configuración de protocolo de enrutamiento común. Por tanto, una estrategia de enrutamiento se relaciona con la ejecución de un solo proceso de enrutamiento para intercambiar actualizaciones y compartir otros parámetros de configuración, como las configuraciones relativas de cada medición de rutas.

Los tres sistemas autónomos de la figura 12-17 podrían estar ejecutando el mismo software de protocolo de enrutamiento (incluso la misma *versión* del mismo protocolo de enrutamiento) pero debido a que los sistemas autónomos no se encuentran dentro del mismo

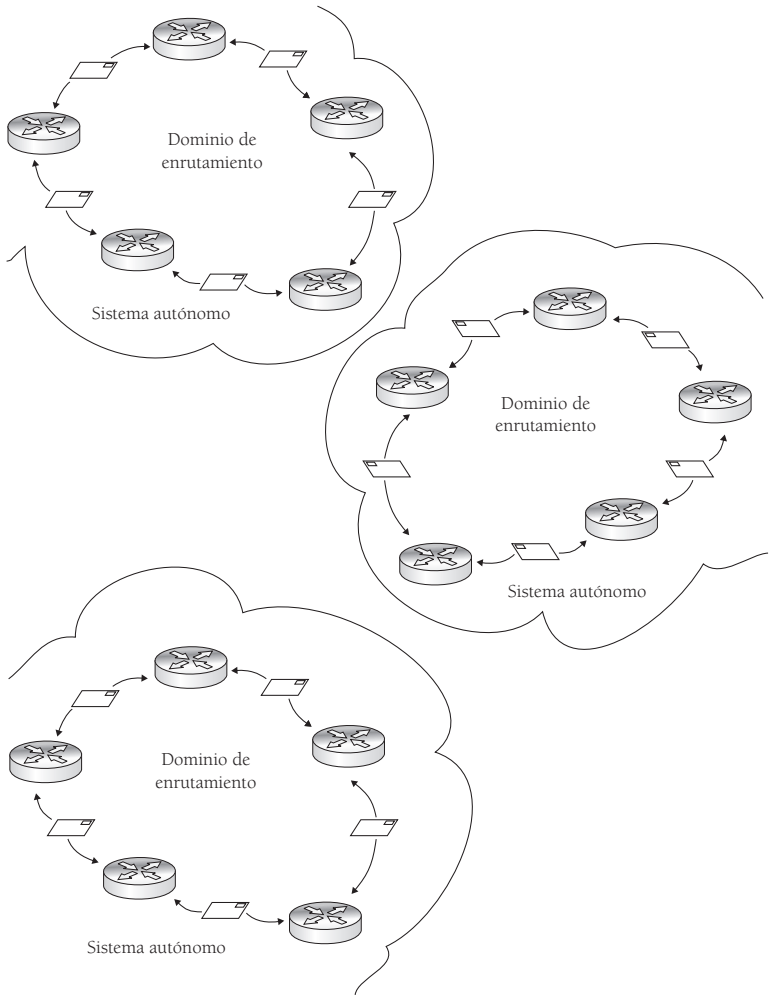
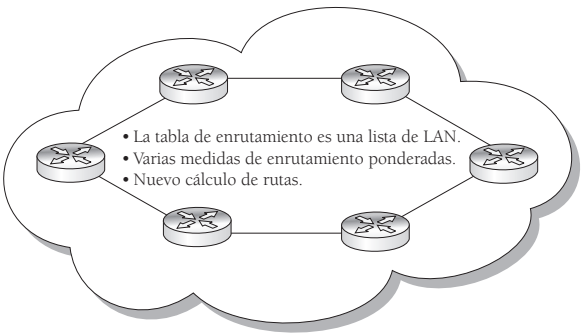


Figura 12-17. Los protocolos de enrutamiento dibujan mapas basados en gran medida en el control administrativo.

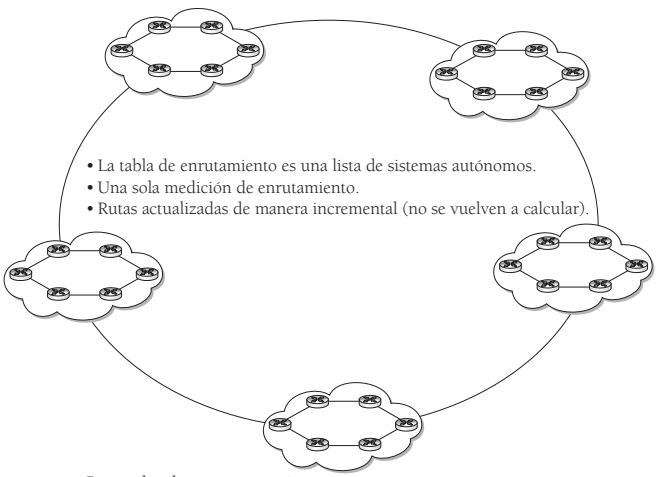
proceso de enrutamiento de los mensajes de actualización y las configuraciones de medición en relativas, no comparten una estrategia de enrutamiento común.

La diferencia entre los protocolos de gateway interiores y exteriores

Así que lo que tenemos entonces es un agradable paquetito donde los dominios de enrutamiento y los dominios administrativos se superponen, ¿verdad? Bueno, como siempre parece ser el caso en las interconexiones, las cosas no son tan simples. Si la estrategia de



Protocolos de gateway interiores.



Protocolos de gateway exteriores.

Figura 12-18. Existen varias diferencias entre los protocolos de gateway interiores y los exteriores.

enrutamiento fuera tan simple como la configuración de un protocolo de enrutamiento para cada dominio administrativo, no habría Internet. Después de todo, si todo fuera interno, ¿quién o qué coordinaría las actualizaciones de enrutamiento entre los millones de sistemas autónomos que conforman Internet?

La respuesta son los protocolos de gateway exteriores. Un *protocolo de gateway exterior* se ejecuta en enrutadores que se encuentran en la orilla de un sistema autónomo e intercambian rutas con otros sistemas autónomos. Estos enrutadores de borde también se denominan *enrutadores de borde*, *enrutadores límite* o *enrutadores de gateway*. Un protocolo de enrutamiento que opera dentro de un sistema autónomo es un *protocolo de gateway interior*. En la figura 12-18 se muestran los dos, lado a lado.

En términos prácticos, la diferencia más obvia entre los dos es donde los enrutadores ejecutan el protocolo en la topología. Los enrutadores exteriores se ubican en la orilla de los

sistemas autónomos; los enrutadores de gateway interiores se ubican hacia la parte media. Una inspección más cercana sobre la manera en que los protocolos exteriores se implementan arroja diferencias más fundamentales:

- ▼ Un protocolo exterior le permite a un sistema autónomo diseñar ciertos enrutadores como pares. El enrutador del borde intercambia actualizaciones con sus enrutadores iguales e ignora otros enrutadores (en protocolos interiores, todos los enrutadores participan en las actualizaciones del enrutador).
- ■ Las tablas de enrutamiento mantenidas por los protocolos exteriores son listas de sistemas autónomos (los protocolos interiores mantienen listas de segmentos de LAN).
- ▲ Los protocolos exteriores simplemente insertan una nueva ruta recibida para un destino en la tabla de enrutamiento; no hay recálculo de las mejores rutas nuevas después de que se recibe una actualización (los protocolos interiores vuelven a calcular nuevas rutas con base en las medidas ponderadas).

Métodos que permiten la interconexión de sistemas autónomos

Llegar más allá de un sistema autónomo invita a los problemas. Para un firewall, el problema potencial es una brecha de seguridad. Para un protocolo de gateway exterior, el problema puede ser mala información acerca de las rutas a los otros sistemas autónomos o sólo demasiada información para manejar. Los problemas heredados en la conexión al exterior también se mantienen para los protocolos exteriores e interiores por igual:

- ▼ Sin alguna manera de filtrar los intercambios de ruta, los protocolos exteriores se verían sobrecargados por una gran cantidad de flujo de tráfico proveniente de Internet.
- ▲ Los protocolos interiores podrían confundirse sobre las mejores conexiones que habrán de tomarse para el exterior sin tener la capacidad de identificar y seleccionar entre los varios orígenes que proporcionan nuevas rutas.

Los protocolos de enrutamiento de gateway interiores y exteriores son un conjunto de técnicas para manejar estos problemas. Como grupo, estas técnicas tienen la intención de reducir el volumen de información de enrutamiento y mejorar la confiabilidad de la información de nuevas rutas que se están recibiendo:

- ▼ **Resumen de ruta** Técnica que divide una interconexión en áreas lógicas, en que el enrutador del borde del área se anuncia sólo a una única ruta de resumen a las otras áreas, con lo que reduce el tamaño de las tablas de enrutamiento.
- ■ **Filtro de rutas** También denominada *distancia administrativa*, una medición de complemento que mide la confiabilidad relativa de las redes individuales como una fuente de la que se pueden aprender rutas óptimas.
- ■ **Etiquetamiento de ruta** Técnica que etiqueta una ruta de varias maneras para identificar el origen del que se aprendió. Las etiquetas pueden incluir el ID del enrutador, el número de sistema autónomo, el ID del protocolo exterior y la medición del protocolo exterior.
- ▲ **Autentificación del enrutador** En efecto, esto requiere que un enrutador de comunicación presenté una contraseña antes de que el enrutador que recibe acepte las actualizaciones de enrutamiento de él.

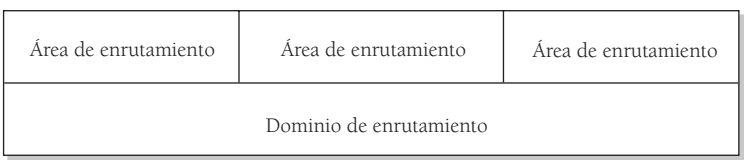
Es notable que algunas de las técnicas estén implementadas en ambos sistemas, los internos y externos no sólo en uno o en otro. Esto se hace para permitir que los dominios de enrutamiento interiores y exteriores actúen en concierto con los flujos de mensajes entre los sistemas autónomos y el mundo exterior. Otro hecho notable es que algunas de estas técnicas se aplican entre los dominios de enrutamiento interior donde diferentes protocolos de enrutamiento se están ejecutando dentro del mismo sistema autónomo (por ejemplo, el resumen de ruta entre los procesos de enrutamiento OSPF y RIP).

Dominios de enrutamiento, áreas de enrutamiento y dominios administrativos

Un *dominio de enrutamiento* es un grupo de sistemas terminales dentro de un sistema autónomo. Un sistema autónomo, a su vez, está definido como un dominio administrativo, donde existe un control administrativo singular sobre directivas y equipo de red.

La mayor parte de las arquitecturas de protocolo de enrutamiento coordinan el intercambio de información de ruta completa entre todos los enrutadores del dominio de enrutamiento. Sin embargo, esta práctica puede volverse ineficiente a medida que crecen las interconexiones, porque eso significa que el tráfico más actualizado viaja distancias más grandes.

Los protocolos de enrutamiento más modernos usan el concepto de áreas de dominio de enrutamiento. Un *área de enrutamiento* es una subdivisión de un dominio de enrutamiento en grupos relacionados lógicamente, en que cada área se identifica de manera única por un nombre o número de área. El principal beneficio de las áreas es que la información de ruta puede resumirse cuando se intercambia entre áreas, reduciendo el excedente de tráfico en la red y mejorando el control sobre el flujo del tráfico. Las áreas de dominio de enrutamiento también se usan para unificar varios dominios de enrutamiento más pequeños en un solo proceso de enrutamiento más grande.



La empresa global típica implementa un solo dominio de enrutamiento en todo el mundo. Esto se hace para que los empleados de un continente puedan conectarse con los colegas de la compañía y los recursos en cualquier lugar del mundo. De esto se desprendería, entonces, que siempre hay una relación uno a uno entre un dominio de enrutamiento y un dominio administrativo. Hasta hace poco, esto era la realidad.

Un nuevo fenómeno llamado redes corporativas externas extiende los dominios de enrutamiento entre dominios administrativos. Una *red corporativa externa* es una configuración en que dos o más empresas construyen un dominio de enrutamiento unificado para compartir rutas entre sus respectivas organizaciones. El dominio de enrutamiento compartido es el subconjunto de cada sistema autónomo general de la empresa, y contiene los recursos y usuarios que habrán de participar en el proceso de negocio compartido. En la figura 12-19 se ilustra la manera en que se instala este tipo de configuración.

Hay que concentrarnos en el caso de las redes corporativas externas en que las rutas se están intercambiando libremente entre empresas (por lo menos dentro del área del dominio

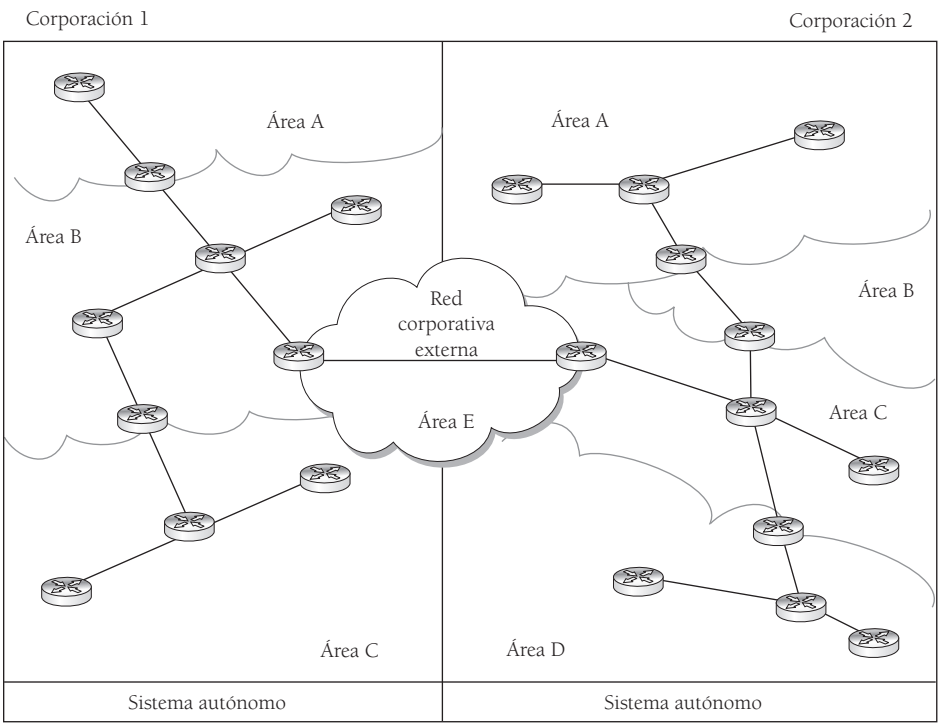


Figura 12-19. Una red corporativa externa es un dominio de enrutamiento entre sistemas autónomos.

de enrutamiento compartido que se encuentra en la parte media). La configuración de red corporativa externa permite a los enrutadores dentro de dos o más empresas mantener un diálogo constante sobre la manera que enruta las conexiones que cruzan los bordes. Ésta es una práctica de interconexión relativamente nueva. No hace mucho, la idea de intercambiar información de ruta directamente entre sistemas autónomos era impensable, no sólo por las preocupaciones por la seguridad de sistema, sino también por razones competitivas.

Ésta es la forma más avanzada de extranet, porque se permite a un *sistema* detrás del firewall de otro. Piénsenlo de esta manera: casi todas las extranet incluyen el inicio de sesión de una persona a través de un firewall al ingresar un nombre de usuario y contraseña. En el ejemplo de la figura 12-19, el sistema de una empresa puede realizar negocios libremente detrás del firewall de otra, de sistema a sistema (no de persona a sistema). Consulte de nuevo la cobertura de los firewall en el capítulo 7, en una red corporativa externa, la extranet está *basada en ruta*, no en *conexión*. Para ponerlo de otra manera, las rutas se comparten entre empresas para uso a largo plazo. En la relación de una extranet tradicional, se permite que un usuario se conecte a un recurso por sesión.

REVISIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO DE CISCO

Cuando la interconexión empezó a despegar a mediados de la década de 1980, las interconexiones eran pequeñas y más simples. El protocolo de gatewary interior que se elegía entonces era Routing Information Protocol (RIP, protocolo de información de enrutamiento). En esa época, las redes de propietario predominantes eran IBM SNA y la implementación de Ethernet DECnet de Digital Equipment, cada una con su esquema de enrutamiento. Pero en esa época, el mercado de red "abierta" estaba despegando, y los servidores Unix se conectaban a las LAN de NetWare IPX de Novell. RIP se incluía con casi todos los sistemas de servidor Unix y emergió como el estándar *de facto*. Por tanto, RIP es un estándar abierto, no una tecnología de propietario de Cisco.

RIP es simple de comprender y fácil de configurar, y funciona para redes pequeñas homogéneas. Al día de hoy, RIP es aún el protocolo de enrutamiento más ampliamente instalado en el mundo.

Pero las versiones iniciales de RIP estaban limitadas sólo a la medición del conteo de saltos. Esto no proporcionaba la flexibilidad de enrutamiento necesaria para administrar entornos complejos. Además, RIP tenía una convergencia lenta y, por tanto, limitada a un conteo de saltos máximo de 16. Configure una ruta más larga y el usuario encontrará un mensaje tipo "destino inalcanzable". Como un protocolo distancia-vector, RIP realiza actualizaciones de enrutamiento a intervalos fijos. (El intervalo de actualización predeterminado para la mayor parte de los productos RIP es de cada 90 segundos.)

Protocolo de enrutamiento de gateway interior de Cisco

Gradualmente se ha vuelto evidente que RIP era una piedra en el camino para la expansión continua de la interconexión. El límite de 16 saltos, el esquema de una sola medición restringía el tamaño de la red y su capacidad. Cisco tomó la oportunidad al idear una tecnología de enrutamiento de reemplazo que superó de parte de las desventajas de RIP: un protocolo distancia-vector más robusto llamado IGRP (Interior Gateway Routing Protocol, protocolo de enrutamiento de gateway interior).

Cisco lanzó por primera vez IGRP, una extensión de propiedad de la compañía del estándar abierto RIP, en 1986 sólo para IP. En los siguientes años, IGRP implementó soporte para otros protocolos en la capa de red (IPX, AppleTalk, etcétera), y se volvió el estándar en las tiendas que usaban sólo equipo de Cisco. Para alrededor de 1990, las limitaciones de RIP se habían vuelto evidentes, e IGRP se estaba posicionado como su reemplazo general para las redes cliente-servidor.

Muchos observadores consideraban que IGRP era el factor único más importante detrás del crecimiento explosivo de Cisco. La competencia había ideado OSPF como su reemplazo principal a RIP, pero estaba limitado (y aún lo está) a redes con sólo IP. La compatibilidad con sólo IP es aceptable en algunas empresas, pero la realidad es que la mayor parte de las interconexiones aún ejecutan varios protocolos (IPX, AppleTalk, DECnet, etcétera). Cisco pudo acoplar funcionalidad superior de IGRP con los internautas que usaban Unix en 1990 para lograr el dominio del mercado del que aún goza.

IGRP era un paso importante porque usaba varias mediciones: distancia, demora, ancho de banda, confiabilidad y carga. Este avance era importante, porque permitió a los ad-

ministradores de red meter mano en una creciente complejidad de red y proporcionar un mejor servicio. En la figura 12-20, se comparan las características de IGRP y de RIP.

Una gran virtud de IGRP es la capacidad de afinar sus mediciones. Por ejemplo, al poder establecer parámetros para confiabilidad o carga en cualquier valor entre uno y 255, da a los administradores la firmeza necesaria para afinar la selección de ruta de IGRP. La capacidad de IGRP para especificar rutas alternas impulsó la confiabilidad y el rendimiento. Eso proporciona redundancia, de modo que si un vínculo deja de funcionar, el algoritmo de enrutamiento de IGRP empieza dinámicamente a dirigir el tráfico a la ruta secundaria. El enrutamiento a través de varios caminos también introdujo el *equilibrio de carga* (la capacidad de desplazar dinámicamente el tráfico hacia rutas alternas, dependiendo de qué tan ocupada estaba cada una). Éstos fueron beneficios importantes durante un periodo en que la mayor parte de las interconexiones estaban en su infancia y propensas a hacerse demasiado lentas o a dejar de funcionar por completo.

En 1994, Cisco aumentó IGRP con un producto llamado Enhanced Interior Gateway Domain Protocol (EIGRP, protocolo mejorado de dominio de gateway interior). EIGRP es un

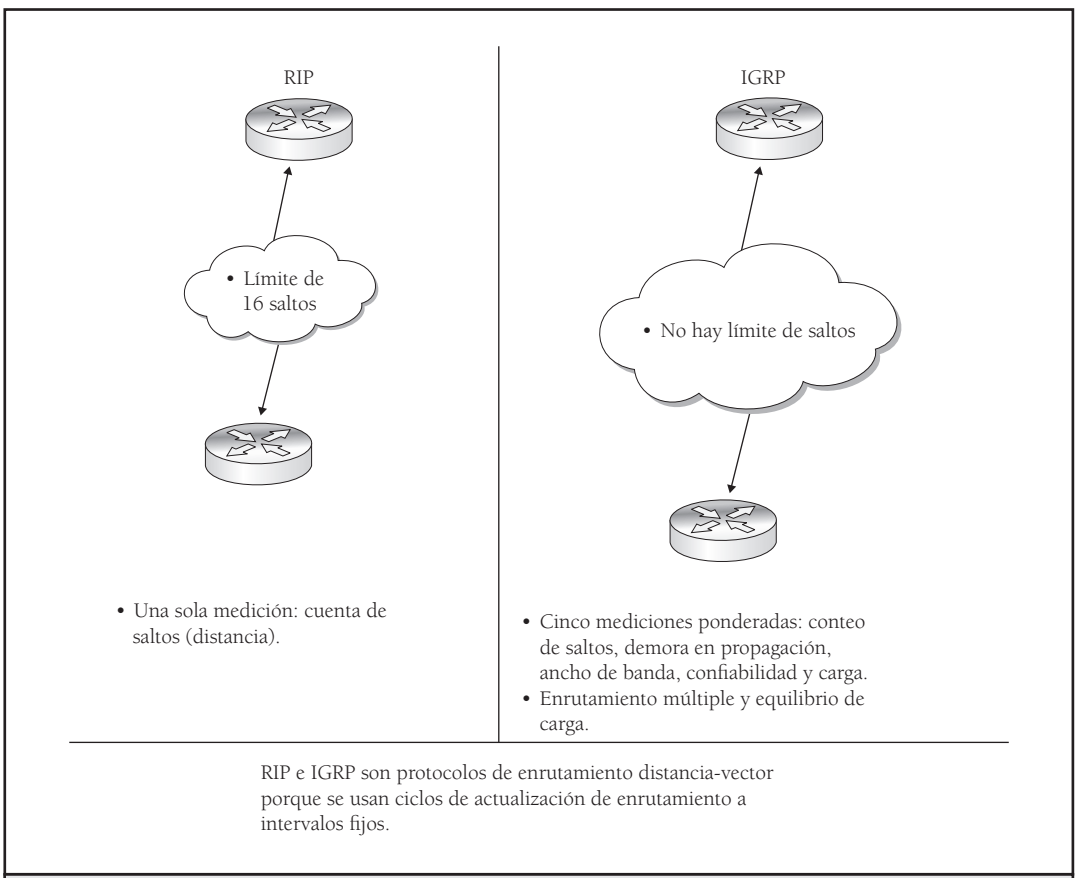


Figura 12-20. IGRP de cisco eclipsó a RIP y ayudó a propulsar a la empresa a lograr una posición de mercado dominante.

avance sustancial sobre su predecesor (tanto como para decir que Cisco pregona que es un protocolo de enrutamiento híbrido en lugar de un simple protocolo de distancia-vector).

EIGRP combina las ventajas de los protocolos de vínculo-estado con los de los protocolos distancia-vector. Proporciona propiedades superiores de convergencia y eficiencia de operación. He aquí las características clave de EIGRP:

- ▼ **Máquina de estado finito DUAL** El motor de software usado por el algoritmo EIGRP. DUAL (Diffusin Update Algorithm, algoritmo de difusión de actualizaciones), se utiliza para proporcionar una operación libre de bucles en cada instante a través de un cálculo de ruta. DUAL permite a los enrutadores sincronizar los cambios de ruta y no incluye enrutadores no afectados por el cambio. La característica clave arquitectónica es que esos enrutadores que ejecutan DUAL almacenan todas sus tablas de enrutamiento vecinas (llamadas *tablas vecinas*) para que puedan volver a calcular de manera más inteligente rutas alternas para acelerar la convergencia.
- ■ **Máscaras de subred de longitud variable (VLSM, Variable-Lenght Subnet Masks)** La capacidad de resumir automáticamente rutas de subred en la orilla de una subred. Antes de VLSM, protocolos de enrutamiento como RIP no podían construir rutas con direcciones de subred incluidas. Todas las subredes tenían que ser iguales.
- ■ **Actualizaciones parciales** También denominadas *actualizaciones disparadas por eventos*, eso significa que las actualizaciones de enrutamiento sólo se miden cuando la topología ha cambiado. Esto ahorra la sobrecarga de mensajes de control.
- ■ **Actualizaciones unidas** El método en que los mensajes de actualización enrutamiento se envían sólo a los enrutadores afectados por el cambio en la topología. Esto ahorra sobrecarga y ayuda a agilizar la convergencia.
- ▲ **Reliable Transport Protocol (RTP, protocolo de transporte confiable)** Un protocolo que garantiza la entrega ordenada de los paquetes de actualización con prioridad a los enrutadores vecinos. RTP funciona al clasificar el tráfico de mensajes de control en cuatro grupos de prioridad: Hello/ACK, actualizaciones, consultas y respuestas, y solicitudes. Sólo las actualizaciones y consultas, las respuestas o ambas se envían de manera *confiable*. Al no enviar Hello/ACK ni solicitudes de manera confiable, los recursos se liberan para garantizar la entrega de los tipos de mensajes más críticos a las operaciones internas de EIGRP.

Es un lugar común para las empresas que usan hardware de Cisco emigrar sus interconexiones de IGRP a EIGRP con el tiempo. Los enrutadores EIGRP pueden operarse de manera compatible con los enrutadores IGRP. Las mediciones entre los dos se traducen de manera directa. EIGRP hace esto al tratar las rutas IGRP como redes externas, lo que permite al administrador de redes personalizar las rutas para ellos. EIGRP anunció tres tipos de rutas:

- ▼ **Rutas internas** Rutas entre subredes en una red adjunta a una interfaz de enrutador. Si la red no está dentro de una subred, no se anuncian rutas interiores para esa red.
- ■ **Rutas de sistema** Rutas a redes dentro del sistema autónomo. Las rutas de sistema se compilan a partir de actualizaciones de enrutamiento pasadas dentro de la interconexión. Las subredes no se incluyen en las actualizaciones de enrutamiento del sistema.

- **Rutas externas** Rutas aprendidas a partir de otro dominio de enrutamiento o las ingresadas en la tabla de enrutamiento como rutas estáticas. Estas rutas se etiquetan de manera individual para rastrear su origen.

En la figura 12-21 se muestra la interrelación entre estos tres tipos de rutas EIGRP. Al dividir las rutas en estas tres categorías se facilitan las funciones avanzadas dentro del algoritmo EIGRP, la designación de rutas internas permite a EIGRP soportar máscaras de subred de longitud variable; las rutas externas permiten que EIGRP intercambie rutas que se descubren fuera del sistema autónomo.

Pasos de configuración general de un protocolo de enrutamiento de Cisco

La configuración de cualquier protocolo de enrutamiento de Cisco es principalmente una cuestión del establecimiento de sus opciones. El número de pasos es una función de cuantas opciones llene el protocolo de enrutamiento para que usted configure. Cuantas más opciones tenga un protocolo de enrutamiento, más comandos podrá usar. Debido a que todos los protocolos de enrutamiento de Cisco están implementados dentro del software IOS, los pasos de la configuración inicial son los mismos. En la tabla 12-1 se explican los pasos de configuración del protocolo de enrutamiento estándar de IOS.

Los dominios de enrutamiento se construyen enrutador por enrutador. En otras palabras, debido a que los protocolos de enrutamiento son arreglos igual a igual, el proceso de enrutamiento debe configurarse en cada enrutador que será incluido en el dominio de enrutamiento. Esto se hace al trabajar de manera individual con cada archivo de configuración del enrutador. Una vez que todos los procesos de enrutamiento estén configurados en todos los enrutadores en la interconexión, estará completo el dominio de enrutamiento.

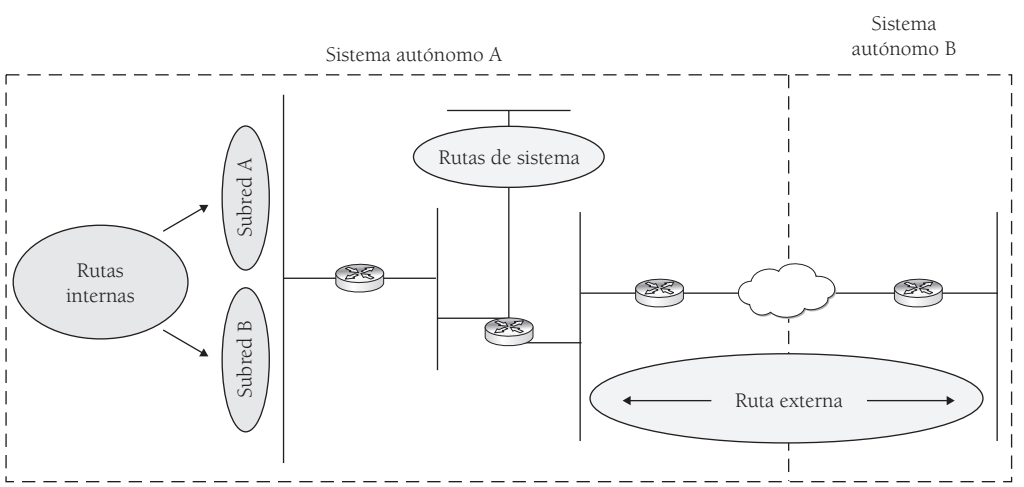


Figura 12-21. EIGRP define tres tipos de rutas: internas, de sistema y externas.

Configuración de EIGRP

El comando **router** inicializa al proceso de enrutamiento en un enrutador. En este ejemplo, un EIGRP para el sistema autónomo 999 está habilitado en un enrutador llamado MyRouter:

```
Myrouter(config)#router eigrp 999
MyRouter(config-router)#
```

Debe darse un número de sistema autónomo para empezar un proceso de enrutamiento. IOS usa el número de sistema autónomo para distinguir un proceso de enrutamiento de otro. Observe que el indicador de comandos de IOS cambió a MyRouter(config-router)# cuando el proceso de enrutamiento **eirp 999** fue invocado. Todos los parámetros del protocolo de enrutamiento están establecidos a partir de este indicador.

El comando **network** se usa para iniciar el protocolo de enrutamiento que se ejecuta en las redes específicas. La red debe estar conectada a una interfaz correspondiente en el enrutador. Al apegarse más a nuestro ejemplo, el siguiente comando haría a la red 10.1.13.0 parte del proceso de enrutamiento:

```
MyRouter(config-router)#network 10.1.13.0
```

El comando anterior inicializa EIGRP en la red 10.1.13.0. Si MyRouter es un gran enrutador de cuatro puertos y los otros tres segmentos LAN también están ejecutando EIGRP, el comando **network** debe usarse para hacerlos también parte del proceso de enrutamiento **eigrp 999**:

```
MyRouter(config)#network eigrp 999

MyRouter(config)# network 10.1.14.0

MyRouter(config)# network 10.1.15.0

MyRouter(config)# network 209.168.98.32
```

Paso de configuración	Descripción
Inicializa y enumera el proceso de enrutamiento.	El protocolo de enrutamiento debe estar ejecutándose en un enrutador para que pueda empezar el intercambio de actualizaciones de enrutamiento con otros enrutadores. Esto se hace utilizando el comando **router** y dando al nuevo dominio de enrutamiento un número de sistema autónomo.
Configura LAN en el dominio de enrutamiento.	El comando **network** se usa para configurar las redes en el dominio de enrutamiento.
Establece otros parámetros del protocolo de enrutamiento.	Una vez que el dominio de enrutamiento está construido, su comportamiento es especificado al usar los diversos comandos del protocolo de enrutamiento a partir del indicador de comandos (config-router)#.

Tabla 12-1. Pasos iniciales para configurar los protocolos de enrutamiento de Cisco.

Ahora el proceso de enrutamiento EIGRP está ejecutándose en los cuatro segmentos LAN de MyRouter, las subredes 10.1.13.0-10.1.15.0 y la red 209.168.98.32.

Cada protocolo de enrutamiento tiene su propio conjunto de comandos. Estos comandos reflejan las capacidades particulares del protocolo. Una vez que el protocolo de enrutamiento se inicializa, sus comandos se usan para establecer varios parámetros en el archivo de configuración para afinar el comportamiento del proceso de enrutamiento a medida que opera en ese enrutador. El comando de EIGRP establecido aparece en la lista de la tabla 12-2.

Dado que esta es una guía de introducción no queremos adentrarnos en los comandos para EIGRP ni en otros protocolos de Cisco (cada uno tiene su propio manual de referencia de comandos completo). Pero al revisar los comandos de la tabla 12-2 le da a una noción de la manera en que los conceptos introducidos en este capítulo se implementan. Tomemos un ejemplo de un comando avanzado para darle una idea de cómo funciona:

```
MyRouter(config-router)#metric maximum-hops 25
```

Lo que hace el comando anterior es establecer un diámetro máximo de la red para el dominio de enrutamiento. El diámetro de red es un límite de cuántos saltos puede dar una ruta antes de que el protocolo de enrutamiento deje de anunciarlo. El establecimiento de este uso del comando **maximun-hops** impondrá un límite de 25 saltos. En caso de que el enrutador

Comando EIGRP	Descripción
auto-summary	Permite el resumen automático de números de red.
default	Establece un comando en sus opciones predeterminadas.
default-information	Controla la distribución de información predeterminada.
default-metric	Establece la medición de rutas redistribuidas.
distance	Define una distancia administrativa.
distribute-listeigrp	Filtra redes en actualizaciones de enrutamiento (usadas con comandos que son específicos de EIGRP).
maximum-paths	Reenvía paquetes en varias rutas.
metric	Modifica las mediciones y los parámetros de enrutamiento de IGRP.
neighbor	Especifica un enrutador vecino.
network	Habilita el enrutamiento en una red IP.
offset-list	Suma o resta el desplazamiento de las mediciones de IGRP o RIP.
passive-interface	Suprime las actualizaciones de enrutamiento de una interfaz.
redistribute	Información de redistribución de otro protocolo de enrutamiento.
timers	Ajusta los cronómetros de enrutamiento.
traffic-share	Calcula la participación en el tráfico para rutas alternas.
variance	Controla la variación en el equilibrio de carga.

Tabla 12-2. Conjunto de comandos de EIGRP.

reciba una actualización de enrutamiento con 26 o más saltos indicados en su medición de distancia, declinará su ingreso en la tabla de enrutamiento. El comando **maximum-hops** es una manera fácil de eliminar el tipo de tráfico que tendrá un enrutador.

Configuración de RIP 2

Aunque las fuertes limitaciones de las versiones iniciales de RIP abrieron la puerta para EIGRP, la competencia regresó a la lucha. La Internet Engineering Task Force (IETF) supervisó el lanzamiento del estándar abierto RIP 2 en 1998. RIP 2 tiene la mayoría de la funcionalidad avanzada de otros protocolos de gateway interiores más modernos como EIGRP y OSPF. Ninguna de las mejoras son únicas de RIP 2, pero han recorrido una larga distancia hacia la captura de la funcionalidad de RIP con otros protocolos de enrutamiento. La EITF siente que esto es algo bueno porque RIP tiene una base instalada amplia y es aún muy útil para pequeñas interconexiones.

Pero aún con estos avances, el uso de RIP 2 todavía está limitado a interconexiones más pequeñas por su límite de 16 saltos. Además, RIP 2 aún permite actualizaciones de enrutamiento en un ciclo de intervalo físico, lo que causa que su convergencia sea más lenta que la de EIGRP u OSPF.

La configuración de RIP 2 incluye los mismos comandos genéricos como lo hacen otros protocolos de enrutamiento de Cisco, donde los comandos deben usarse para inicializar el proceso de enrutamiento en el enrutador y sus redes:

```
MyRouter(config)#router rip
MyRouter(config-router)#network 209.11.244.9
```

Observara que no se introdujo un número de sistema autónomo (como en **router rip 999**), porque ni RIP ni RIP 2 lo soportan. Además, el comando para iniciar RIP 2 es **router rip** (no **router rip2**) porque la versión de RIP que puede ejecutar es una función de la versión de IOS que el enrutador ha cargado. Es decir, la versión de RIP está definida por la ejecución del comando de la versión del modo de configuración del enrutador.

```
MyRouter(config-router)#version ?
  <1-2> version
```

Una vez que es lanzado el proceso de RIP 2, configurarlo es simplemente cosa de establecer sus otros parámetros. En RIP 2 esto incluye la autentificación del enrutador utilizando el comando **rip authentication**, el resumen de la ruta utilizando el comando **auto-summary** y la validación de la dirección IP de los enrutadores en que envían actualizaciones de enrutamiento utilizando el comando **validate-update-source**.

Echemos un vistazo a un ejemplo del comando RIP 2 que es más genérico por naturaleza. El comando **timers basic** se usa para establecer los intervalos de actualización de enrutamiento dentro de un dominio de enrutamiento RIP. La opción predeterminada en los intervalos es de 30 segundos. Si se quiere cambiar la frecuencia de actualización de enrutamiento a cada 25 segundos, se ingresaría el siguiente comando:

```
MyRouter(config-router)#Timers Basic 25
```

Sin embargo, no se recomienda que cambien las mediciones básicas como en este caso. Hacer actualizaciones cada cinco segundos ayudará con más frecuencia a agilizar la convergencia. Pero aumentará la sobrecarga de red al causar más mensajes de enrutamiento.

Configuración de Open Shortest Path First

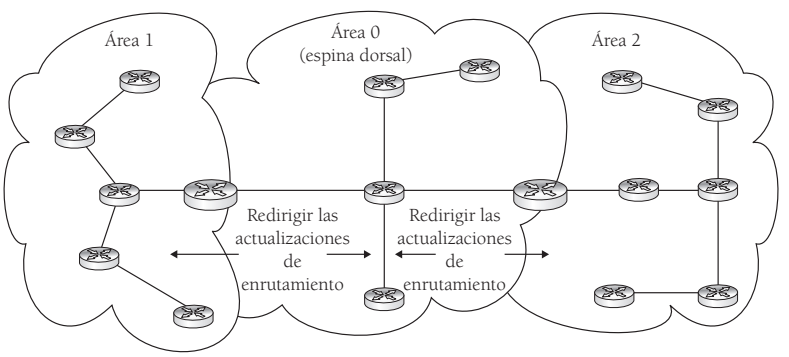
En 1991, la industria se movió a establecer lo que sería llamado un reemplazo de estándar abierto para RIP. El resultado fue OSPF (abra primero la ruta más corta), que, como su nombre lo indica, es un estándar abierto utilizado para buscar las rutas más cortas de la misma manera que RIP. Pero ahí es donde terminan las similitudes. OSPF es un protocolo de enrutamiento vínculo-estado, no distancia-vector. OSPF converge más rápido que RIP y opera bajo el concepto de vínculo-estado, en que cada enrutador mantiene una base de datos de todos los vínculos en una red y la información sobre cualquier demora que podría experimentarse. Además, ASPF ahorra sobrecarga de mensajes de control al emitir actualizaciones de enrutamiento sólo bajo una base orientada a eventos.

Áreas de enrutamiento de OSPF

La mayor parte de las características de OSPF están diseñadas para ayudar a tratar con el tamaño de la interconexión. El concepto central detrás de OSPF son las áreas de interconexión. Como se estableció al principio de capítulo, un área es una zona dentro de un sistema autónomo que está integrada por un conjunto lógico de segmentos de red y sus dispositivos conectados. El sistema de enrutamiento utiliza las áreas como una estrategia para el flujo de tráfico de control y para dejar fuera los detalles de la tabla de enrutamiento indeseables. Cada dominio OSPF debe tener un área de espina dorsal con el 0. Las áreas se crean al utilizar la palabra clave **area** como argumento con el comando **network**, como se muestra a continuación:

```
MyRouter(config-router)#network 10.0.0.0 0.255.255.255 area 0
```

Ese comando pone la subred 10.0.0.0 en el área 0 de OSPF. Es posible ejecutar una red OSPF de un área, teniendo sólo un área 0. En la figura 12-22 se muestra una red OSPF de tres áreas.



Los enrutadores A y B de los límites del área redirigen las actualizaciones de enrutamiento entre las áreas de dominio del enrutamiento OSPF.

Figura 12-22. OSPF implementa áreas de enrutamiento y redirige las rutas entre ellas.

Una funcionalidad clave de OSPF es que puede redirigir las actualizaciones de enrutamiento entre áreas. *Redirigir* es una actualización de enrutamiento que pasa a través de una o más áreas de un dominio de enrutamiento, por lo general a través de varios filtros diseñados para cortar el tráfico de actualización enrutamiento.

Las redes OSPF suelen usarse para unir dominios de enrutamiento preexistentes, como interconexiones RIP. Esto se hace al crear un área para cada dominio RIP y pasando actualizaciones de enrutamiento entre ellas a través de la espina dorsal OSPF (área 0). Los enrutadores en las orillas de las áreas son denominados Autonomous System Boundary Routers (ASBR, enrutadores de límite de sistema autónomo). Los ASBR se establecen entre los sistemas autónomos OSPF y las redes RIP, y ejecutan los protocolos OSPF y RIP.

Máscaras de subred de longitud variable

El soporte Variable-Lenght Subnet Mask (VLSM, máscara de subred de longitud variable) es una característica crítica para OSPF. Las áreas respectivas tienen sus propios esquemas de subred que satisfacen sus particulares necesidades. En la figura 12-23 todas las redes de base de línea serial en el área 0 usan la máscara de subred .252, típica para conexiones de gran distancia. Esto es porque la mascara .252 permite hasta 64 subredes, pero sólo dos hosts por subred. Mientras que la máscara de subred podría variar, con base en un conjunto determinado de requisitos, esto es ideal para las redes compuestas por una conexión de línea serial porque sólo se necesitan dos host: uno en cada extremo de la línea.

Cada una de las otras áreas del extremo del sistema usa su propio esquema. El área 1 usa la máscara .248 (lo que arroja un máximo de 32 subredes con seis hosts cada una), el área 2 usa la máscara .192 (hasta cuatro subredes y 62 hosts cada una), y el área 3 usa la máscara .224 (hasta ocho subredes con 30 hosts cada una).

VLSM soporta medios que todas las rutas intercambiadas en actualizaciones pasadas entre las áreas de OSPF pueden incluir las direcciones de subred (en lugar de sólo las direcciones de éstas). Ésta es una característica importante, porque permite que se compartan rutas completas entre áreas utilizando diferentes esquemas de subred, lo que significa que cada área puede usar sólo la cantidad de espacio de dirección requerido para sus necesidades. Por ejemplo en el área 0 de la figura 12-23, sólo hay unos cuantos hosts conectados a las líneas seriales, y el poder usar las máscaras .248 le permite al área 0 usar sólo unas cuantas direcciones (una máscara .248 sólo tiene seis hosts por subred).

Aún con todo el poder de OSPF, sería difícil escalar el tamaño de una interconexión en gran medida sin VLSM. Eso se debe a que casi todas las LAN usan esquemas de dirección de subredes para conservar el precioso espacio de dirección IP. Las áreas OSPF hacen posible la expresión a gran escala de los dominios de enrutamiento y, por tanto, el tamaño de la interconexión. VLSM permite a los enrutadores tener una visibilidad completa de dirección entre áreas y, por tanto, en ruta el tráfico dentro de las interconexiones con mucha mayor eficiencia.

Protocolo de gateway de borde

El Border Gateway Protocol (BGP, protocolo de gateway de borde) es el protocolo de enrutamiento de alto nivel que hace posible Internet. Optimizado para coordinar la interconexión entre sistemas autónomos, BGP es, en este punto, casi el único protocolo de gateway exterior en uso hoy en día.

Existen varias versiones de BGP, y el IOS de Cisco los soporta todos. La versión dos de BGP está definida en el RFC 1267, y la versión cuatro en el RFC 1771. Vale la pena que

lo lean quienes están interesados en profundizar en BGP. Pero por ahora, mantengámoslo sobre el piso.

EIGRP y OSPF permiten que los operadores de red escalen sus interconexiones a grandes capacidades, pero es BGP el que los une a lo largo de las llamadas troncales de Internet o redes de igual a igual. Casi ningún tipo de red trabajará con BGP; su uso se deja principalmente a los administradores de ISP preocupados con el descubrimiento de rutas a través de espinas dorsales de alta velocidad. Sin embargo, es útil revisar brevemente la manera en que se usa BGP.

La predominancia de un solo protocolo de enrutamiento exterior no es sorpresiva a la luz del hecho de que los operadores de red en el mundo necesitan un solo estándar para integrar los millones de sistemas autónomos que operan en el mundo. Si la industria no hu-

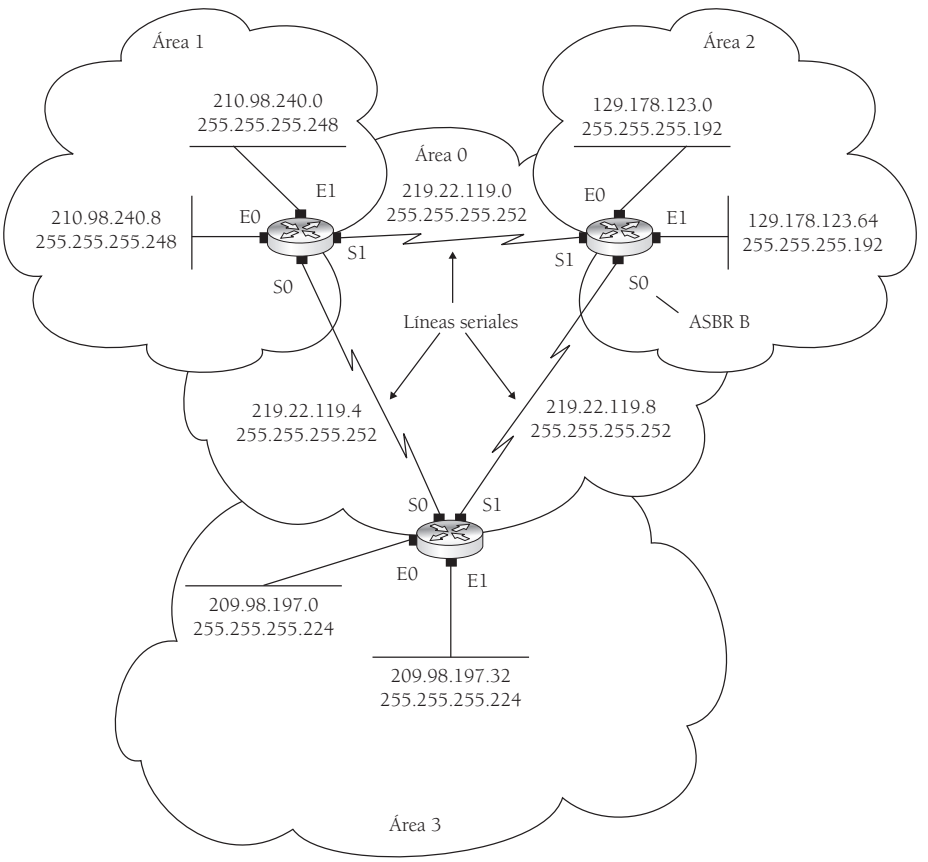


Figura 12-23. La característica de máscara de subred de longitud variable permite la creación de áreas.

biera establecido BGP como la plataforma común, algún otro protocolo de exterior gateway sería en cambio el estándar *de facto*.

Enrutamiento BGP

Como los de gateway interiores, BGP puso los mensajes de actualización de enrutamiento y las mediciones para mantener las tablas de enrutamiento. BGP es un protocolo de enrutamiento de arquitectura vínculo-estado, pero obviamente es radicalmente diferente en arquitectura para que pueda escalar al crecimiento de Internet. La arquitectura de BGP está caracterizada por el uso de la delegación de ruta y la capacidad de trabajar con los protocolos de gateway interior. BGP soporta tres tipos de enrutamiento:

- ▼ **Sistema interautónomo** El enrutamiento de sistema interautónomo es la función básica de BGP en las operaciones de enrutamiento de Internet.
- ■ **Sistema intra-autónomo** El enrutamiento de sistema intra-autónomo es realizado por BGP cuando dos o más enrutadores BGP operan dentro del mismo sistema autónomo. A esto generalmente se le ve en casos en que es necesario cruzar una interconexión larga de un extremo al otro.
- ▲ **Sistema autónomo de paso** El enrutamiento de sistema autónomo de paso ocurre cuando es necesario que el tráfico de BGP atraviese un sistema autónomo que no es de BGP para conectarse a otro sistema autónomo de BGP.

Como un protocolo de enrutamiento de gateway exterior optimizado para escalar el tamaño de Internet, BGP difiere fuertemente de los protocolos interiores de algunas maneras fundamentales:

- ▼ **Enrutadores de igual e igual** Los administradores de red especifican una lista de enrutadores BGP que presentan otros sistemas autónomos (por lo general otros ISP o portales grandes de interconexión). Esto se hace porque no es factible pasar actualizaciones de enrutamiento a través de dominios de enrutamiento en todo el mundo.
- ■ **Contenido de tabla de enrutamiento** Una entrada de tabla en BGP es un sistema autónomo (no una LAN, porque es un protocolo de gateway interior). Cada ruta consta de un número de red y una lista de sistemas autónomos por los que debe pasarse, llamado una ruta AS.
- ■ **Medición única de enrutamiento** BGP utiliza una sola medición para determinar la mejor ruta a una red determinada. Esta medición consta de un número arbitrario para ponderar el grado de preferencia por un vínculo determinado. No es dinámica; un administrador de redes debe ingresar la información y actualizarla.
- ▲ **Actualizaciones de ruta incrementales** Cuando se recibe una actualización de enrutamiento, BGP simplemente reemplaza la ruta anterior con la nueva. No se hace un mejor recálculo de ruta, porque para mantener una base de datos vínculo-estado en la topología de Internet no es factible.

La implementación de Cisco de BGP soporta que cada enrutador establezca un conjunto de vecinos, o colegas, con los cuales intercambiaron información de accesibilidad. Se utilizan diversas técnicas para agregar rutas que ayuden a simplificar el procesamiento de rutas y a reducir el tamaño de las tablas de enrutamiento. Uno es el uso de los *mapas de ruta* (una práctica que restringe la diseminación de actualizaciones de enrutamiento a ciertos enrutadores). Otra es el uso de una forma simplificada de distancia administrativa, donde, en lu-

gar de tener la elección entre 255 ponderaciones relativas, una ruta puede tomar cualquiera de tres calificaciones confiables, dependiendo de la posición en la topología del enrutador.

La faceta clave de BGP es la capacidad de filtrar, reducir y simplificar la información de enrutamiento que se reúne de Internet.

Conmutación de etiquetas de varios protocolos

Otra manera de enrutar paquetes a través de una interconexión es con un protocolo que delinie todo el proceso. Multiprotocol Label Switching (MPLS, conmutación de etiqueta de varios protocolos) es una manera de reenviar paquetes a través de una interconexión. Los enrutadores situados en la orilla de una red aplican etiquetas simples a los paquetes. Luego los enrutadores, conmutadores, otros dispositivos de red dentro de la red pueden conmutar paquetes con base en las etiquetas. Ese proceso es ideal, porque requiere un mínimo de trabajo excedente de búsqueda.

Cómo funciona

El enrutamiento IP convencional de capa tres está basado en el intercambio de la disponibilidad de información de la red. A medida que un paquete se abre camino por la red, cada enrutador toma decisiones acerca de dónde enviará a continuación el paquete. Esta información se basa en la información que hay en la capa tres del encabezado, y se usa como índice para la búsqueda de una tabla de enrutamiento que determine el siguiente salto del paquete. Ese proceso se repite en cada enrutador de la red. A cada salto, el enrutador tiene que resolver el siguiente destino del paquete.

La desventaja de este proceso es que la información dentro de los paquetes IP (como la información acerca de la precedencia o de los datos de VPN, por ejemplo) no se considera cuando se reenvían los paquetes. Para un mejor desempeño, sólo se toma en consideración la dirección de destino, pero, debido a que otros campos dentro del paquete pudieran ser relevantes, un análisis a profundidad del encabezado debe tener lugar en cada enrutador a lo largo de la ruta del paquete.

MPLS delínea este proceso al colocar una *etiqueta* en cada paquete. Considere el enrutamiento IP convencional como la dirección de una carta. Le indica a la oficina postal a donde enviarla. MPLS lleva la dirección a otro nivel al agregar instrucciones adicionales (como escribir "perecedero" o "no doblar" en el sobre).

La etiqueta incluye información importante acerca del paquete, incluida:

- ▼ Destino.
- ■ Precedencia.
- ■ Una ruta específica para el paquete, si es necesaria.
- ■ Membresía de red privada virtual.
- ▲ Información de calidad de servicio (QoS).

MPLS causa que el análisis del encabezado de capa tres se ha realizado sólo dos veces: en el Label Switch Router (LSR, enrutador de conmutación de etiqueta) a medida que entra y sale de la interconexión. En el LSR, el encabezado de capa tres se asigna a una etiqueta de longitud fija y se aplica al paquete. En la figura 12-24 se muestra la manera en que se aplica una etiqueta a un paquete.

El encabezado MPLS de 32 bits contiene los siguientes campos, tal como están numerados en la figura 12-24:

1. El campo de la etiqueta (20 bits) contiene el valor real de la etiqueta MPLS.
2. El campo Class of Service (CoS, clase de servicio) de 3 bits puede afectar la disposición en cola, y descartar algoritmos aplicados al paquete a medida que se transmite en la red.
3. El campo Stack (S, pila) de 1 bit soporta una pila de etiqueta jerárquica.
4. El campo TTL (time-to-live, tiempo de vida) de 8 bits proporciona funcionalidad IP TTL convencional.

A continuación, a medida que el paquete cruza los enrutadores de una interconexión, sólo las etiquetas necesitan leerse. Una vez que alcanza el otro extremo de la red, otro LSR de extremo elimina la etiqueta, reemplazándola con los datos de encabezado apropiados para esa etiqueta.

Una clave resultante de este argumento es que las decisiones del envío basadas en alguno o en todos estos diferentes orígenes de información pueden alcanzarse por medio de una sola búsqueda de tabla a partir de una etiqueta de longitud fija. La conmutación de etiquetas es la combinación de las funciones de conmutación y enrutamiento (combina la información de disponibilidad de los enrutadores con los beneficios de la ingeniería de tráfico de los conmutadores).

Beneficios

MPLS ofrece muchas ventajas sobre el IP tradicional y los protocolos de enrutamiento ATM, la conmutación de etiquetas y la conmutación de hardware funcionan juntas para entregar grados elevados de rendimiento. Para las redes de multiservicio, MPLS permite que un conmutador proporcione ATM, Frame Relay y servicio IP en una sola plataforma. Esto es ideal, porque el soporte de todos estos servicios en una sola plataforma no sólo es costeable, sino que también simplifica el suministro para los proveedores de varios servicios.

Y aparte de los siguientes beneficios resaltan algunas de las utilidades de MPLS:

- **Integración** MPLS combina la funcionalidad de IP y de ATM haciendo que la infraestructura de ATM sea visible para el enrutamiento IP y eliminando la necesidad de asignaciones entre las características de IP y ATM.
- **Rendimiento de VPN** Con una espina dorsal MPLS, la información de VPN sólo necesita procesarse donde los paquetes entran y salen de la red. Además, se usa BGP

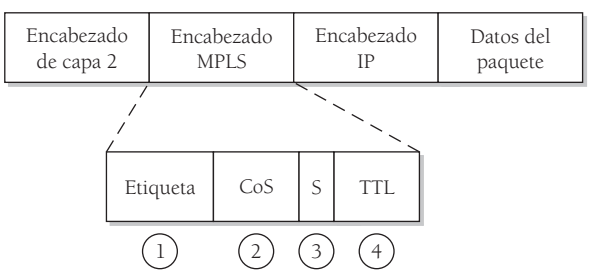


Figura 12-24. Los paquetes MPLS contienen siete campos.

para tratar con información de VPN. El uso de MPLS y BGP hace que los servicios VPN basados en MPLS sean más fáciles de manejar y mucho más escalables.

- **Reducción de la carga en servicios esenciales** Debido a que MPLS examina paquetes cuando entran y salen de una red, los enrutadores de tránsito interno y los conmutadores sólo necesitan procesar la conectividad con los enrutadores de orilla del proveedor. Esto evita que los dispositivos esenciales se vuelvan sobrecargados con el volumen de enrutamiento intercambiado en Internet.
- **Capacidades de ingeniería de tráfico** Las capacidades de ingeniería de tráfico de MPLS permiten a los administradores de red desplazar la carga de tráfico de las secciones sobrecargadas a las que tienen poco uso de la red, con base en el destino de tráfico, el tipo, la carga y la hora del día.

La estructura de la red MPLS

Una red MPLS tiene tres componentes básicos. Son:

- **Enrutadores de conmutación de etiquetas de orilla** Los LSR de orilla están situados en los límites físicos y lógicos de una red. Estos dispositivos suelen ser enrutadores (como el Cisco 8500), pero también pueden ser conmutadores LAN de varias capas (como el Cisco Catalyst 6500) o un dispositivo proxy.
- **Conmutadores de etiqueta** Estos dispositivos conmutan paquetes con base en las etiquetas. Además, los conmutadores de etiqueta también pueden soportar enrutamiento de capa tres o de capa dos. Algunos conmutadores de etiqueta se incluyen en Cisco 6500, Cisco 8540 Multiservice Switch Router y el Cisco 8500.
- **Protocolo de distribución de etiquetas** El Label Distribution Protocol (LDP) se usa en todo los protocolos de enrutamiento de capa de la red y distribuye información de etiqueta entre dispositivos de redes MPLS.

MPLS proporciona interconexiones con un nivel sin precedentes de control sobre el tráfico, lo que da como resultado una red más eficiente, que soporta servicios más predecibles y que puede ofrecer la flexibilidad requerida para cumplir constantemente con situaciones de red cambiantes.

Estrategia de protocolos de enrutamiento de Cisco

El movimiento realizado alrededor de 1990 para reemplazar RIP con un protocolo de gateway interior más robusto fue un movimiento clave en la historia de la industria de las interconexiones. (Tenga en cuenta que en 1990 es una fecha muy remota en el tiempo de Internet.) La capacidad para escalar más allá de 16 saltos o un diámetro de red de 50 enrutadores apenas era necesaria. Una convergencia más rápida también estaba en la lista crítica, porque los bucles se estaban convirtiendo un problema que presionaba.

Cisco explotó el momento al promover IGRP como un reemplazo de RIP. Eso fue un riesgo, porque IGRP era (y es) un estándar de propietario. Pero la estrategia tuvo gran éxito, porque resolvió las necesidades de los clientes de una expansión continua de la interconexión, y al mismo tiempo, persuadió a los administradores de redes a estandarizar a partir del equipo de Cisco. Casi todos los que hicieron eso han mirado desde entonces a EIGRP.

OSPF es un protocolo de enrutamiento que sólo usa IP. Quienes planean la tecnología en el grupo de trabajo de OSPF tenían razón en promover un reemplazo de RIP. Y probable-

mente tenían razón en que un día todas las redes estarán basadas en el protocolo Internet, pero eso no sucederá en los próximos 10 años. Fue sólo hace 10 años que muchos estaban señalando con el dedo a Novell y se quejaban de que mantenía un monopolio en los sistemas operativos LAN de cliente-servidor. Hay millones de LAN IPX a la fecha. La realidad es que casi todas las empresas aún tienen una mezcla de protocolos en el nivel de la red y necesitan soporte para ellos utilizando un protocolo de gateway interior como EIGRP. Ésta fue la ventana de mercadotecnia que Cisco explotó.

Cisco soporta un producto OSPF, como complemento de su estrategia de EIGRP. OSPF es un producto importante por derecho propio. Casi todos los ISP (y un creciente número de empresas) están ejecutando grandes dominios de enrutamiento que sólo usan IP, y dado el establecimiento de estándares de Internet, muchos consideran que un día, todos usarán únicamente IP. OSPF ha construido la infraestructura crítica para la misión rodeando y sosteniendo las redes de igual a igual BGP. Sin OSPF, estas redes tal vez ya no serían posibles. Ambas están habilitando tecnologías que hicieron posible el explosivo crecimiento de las interconexiones y de Internet. Además EIGRP e IGRP sólo se usan en entornos que incluyen sólo equipo de Cisco. Cuando se agrega a la red equipo de otros comercializadores, OSPF se vuelve importante.

Más aún, el soporte de Cisco a MPLS delínea el enrutamiento a través de las interconexiones. Como hemos visto, al modificar un encabezado en un paquete cuando entra en su red, y luego podarlo, MPLS mejora la funcionalidad de la red y facilita la carga en dispositivos de red centrales. El uso de MPLS es ciertamente benéfico cuando se incluyen los temas de rendimiento y capacidad de la red.

La comparación de la funcionalidad de los protocolos de enrutamiento actuales puede resultar confusa. Aunque RIP es el menos importante de los protcolos de gateway interiores, se ha mejorado tanto que ahora comparte mucha de la funcionalidad avanzada disponible con EIGRP y OSPF. Para confundir aún más el panorama de los protocolos de enrutamiento RIP y otros protocolos están incluyéndose en dominios OSPF como áreas de dominio de enrutamiento. Las cosas se han nublado aún más porque OSPF es tan escalable que tiene una gran funcionalidad de ampliación de tamaño relacionada con BGP.

Basta decir que los protocolos de enrutamiento de hoy en día se superponen tanto que es difícil mantener las cosas simples. Sólo tenga en cuenta que las distinciones esenciales son las arquitecturas distancia-vector en comparación con vínculo-estado y protocolos de gateway interiores en comparación con exteriores.

CAPÍTULO 13

Administración de red

Hemos cubierto las principales partes de la tecnología que integran las interconexiones. Los enrutadores, conmutadores, firewalls y servidores de accesos están conectados con cable para formar topologías de red. La mayor parte de las configuraciones usan cables de cobre de par trenzado alimentados en espinas dorsales de fibra óptica, que mueven datos a velocidades de 100 Mbps hasta unos 10 Gbps, que suenan como algo fantástico. Mientras los dispositivos de red varían en tipo y tamaño, la mayoría tiene el aspecto de PC o servidores porque tienen memoria, CPU y tarjetas de interfaz. Sin embargo, carecen de disco, apenas tienen monitor, y usan sus interfaces para conectar redes en lugar de periféricos.

La infraestructura de software de Cisco para hacer que esto funcione incluye varios sistemas operativos como Internetwork Operating System (IOS, sistema operativo de interconexión). IOS es un paquete ligero de comandos, software de protocolo y el importante archivo config. Las imágenes del software IOS difieren en gran medida, dependiendo del tipo de dispositivo. El conmutador tiene una versión modesta del IOS, mientras que el enorme Cisco Gigabit Router de la serie 12000 está cargado de protocolos y paquetes de software de administración especializados. Sin importar el tipo de dispositivo o la funcionalidad del IOS, el comportamiento de la red es controlado al establecer parámetros en el archivo config.

Como vimos en el capítulo anterior, tal vez la tecnología de interconexión más sofisticada de todas es el protocolo de enrutamiento. Los protocolos de enrutamiento le dan a las interconexiones un nivel de conciencia y adaptación propias sin las cuales las configuraciones a gran escala no serían prácticas. Hacen esto al construir una jerarquía de LAN y sistemas autónomos para encontrar rutas óptimas para recorrer el campus de la oficina (o ir al otro lado del mundo).

Sin embargo, se necesitan más que rutas óptimas para ejecutar una interconexión. La capacidad de operar por sí solo es solamente una parte de la ecuación de la administración de red. Los protocolos de enrutamiento pueden tener la capacidad de manejar más problemas minuto a minuto, pero las interconexiones aún requieren constantes esfuerzos de administración por parte de la gente. Sin una revisión persistente y la intervención de los administradores, la capacidad de una interconexión para operar por sí sola sería abrumada por un deterioro progresivo en las condiciones de operación. Las interconexiones deben estar actualizadas constantemente e incluso actualizarse para ajustarse a los problemas, el crecimiento y el cambio. Los equipos de red necesitan herramientas para administrar el cambio y anticiparse a los problemas (y, se espera, que para evitarlos).

Si se dejan solas, aun las interconexiones perfectamente configuradas se degradan bajo la atención de los usuarios añadidos, las cargas aumentadas, el tráfico cambiante, las nuevas versiones de hardware y software, y la nueva tecnología. Los administradores de red deben vigilar, reconfigurar, detectar y solucionar problemas sin fin. El crecimiento reciente en usuarios (y el aumento en la cantidad de tráfico generado por los usuarios) ha dejado a los equipos de red con problemas para mantenerse al día. Los protocolos de enrutamiento y otras características automatizadas sólo hacen que sea factible la administración de las interconexiones, pero no lo hacen fácil. Las herramientas de administración de red también son necesarias. La respuesta de la industria ha sido un flujo de estándares, tecnologías y productos concentrados en la configuración y la operación de interconexiones.

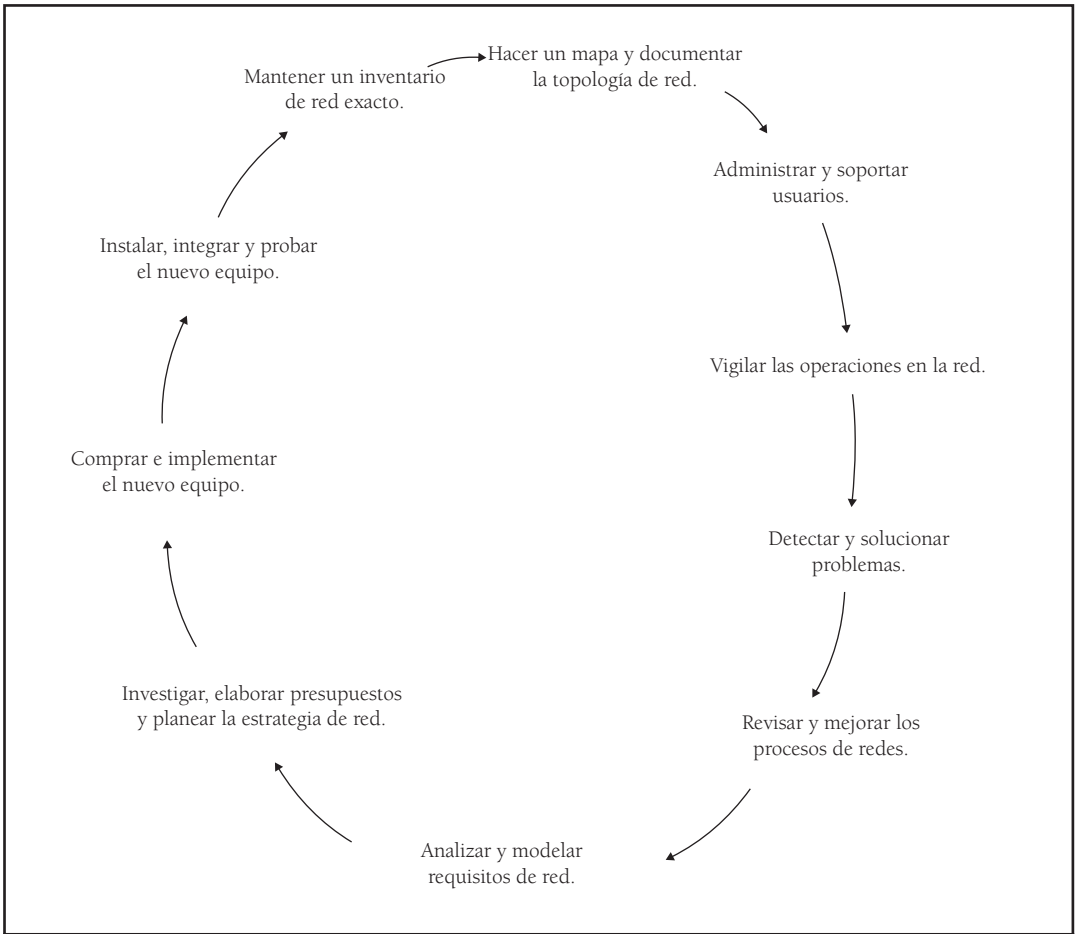


Figura 13-1. Las tareas de la administración de redes siguen un ciclo intensivo.

REVISIÓN GENERAL DE LA ADMINISTRACIÓN DE RED

La administración de red puede confundir a los novatos. Por su naturaleza, el campo incluye listas enormes de datos. En la figura 13-1 se presenta gráficamente el rango de tareas realizadas por el equipo de administración de red típico.

Las interconexiones se deben planear, modelar, presupuestar, diseñar, configurar, comprar, instalar, probar, mapear, documentar, operar, vigilar, analizar, optimizar, ajustar, expandir, actualizar y fijar. Es mucho. Ninguna herramienta puede hacer todas estas cosas, por lo menos aún no. Basta con decir que los productos y los servicios de administración de red son una industria por sí misma, integrada por una compleja serie de tecnologías, productos, y comercializadores que proporcionan todo, desde simples analizadores de protocolo que miden un solo vínculo hasta centros de comando de red mundial.

NOTA Tal vez haya notado que el término "administración de redes" se usa en relación con las interconexiones. (Ya casi nadie maneja sólo una LAN.) El término se sigue usando desde el surgimiento de las interconexiones y aún es de uso universal. No hay una diferencia real entre la administración de redes y la administración de interconexiones.

La evolución de las herramientas de administración

Históricamente, el problema con las herramientas de administración de computadoras ha sido el soporte real de varios comercializadores. En otras palabras, es difícil encontrar una sola herramienta que pueda manejar equipo de diferentes fabricantes con la misma calidad. Es difícil mantener las configuraciones de varios comercializadores (la norma en casi todas las infraestructuras de tecnología de la información empresariales de hoy en día) empleando una sola herramienta debido a las sutiles diferencias en el equipo de cada fabricante.

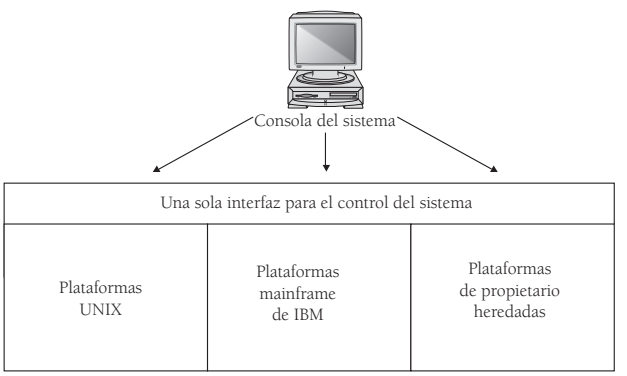
Las herramientas de administración de computadoras han evolucionado desde polos opuestos de la industria de la computación: sistemas y redes. El objetivo es atraer todos los activos computacionales bajo el control de la administración de una sola herramienta, y el predominio de la colocación de sistemas hosts en redes está conduciendo a los sistemas existentes y a las herramientas de administración de redes hacia los brazos de otros.

Consolas tradicionales de administración de sistemas

Los sistemas de administración de computadoras sofisticados llamados *consolas de sistema* han existido durante décadas. Estas consolas generalmente se conectaban a mainframes instalados en un centro de datos y usados para programar trabajos, realizar copias de seguridad y corregir problemas. Con el tiempo, desarrollaron más y más capacidades, como la administración de computadoras remotas.

El producto mejor conocido del molde del centro de datos es Unicenter de Computer Associates (CA). Unicenter es actualmente una amalgama de productos que se ha unido en una sola solución de administración. Unicenter evolucionó de ser una consola sofisticada para la administración de mainframes de IBM y grupos de discos, a un sistema de administración integrado con soporte para todas las plataformas de hardware y software importantes. La mayor parte del crecimiento del producto Unicenter se ha logrado mediante la adquisición, lo que es comprensible dado el alcance del producto.

La clave a Unicenter y otras consolas de sistema es la capacidad de manejar las varias arquitecturas de computación que es probable que las empresas pongan en una configuración.

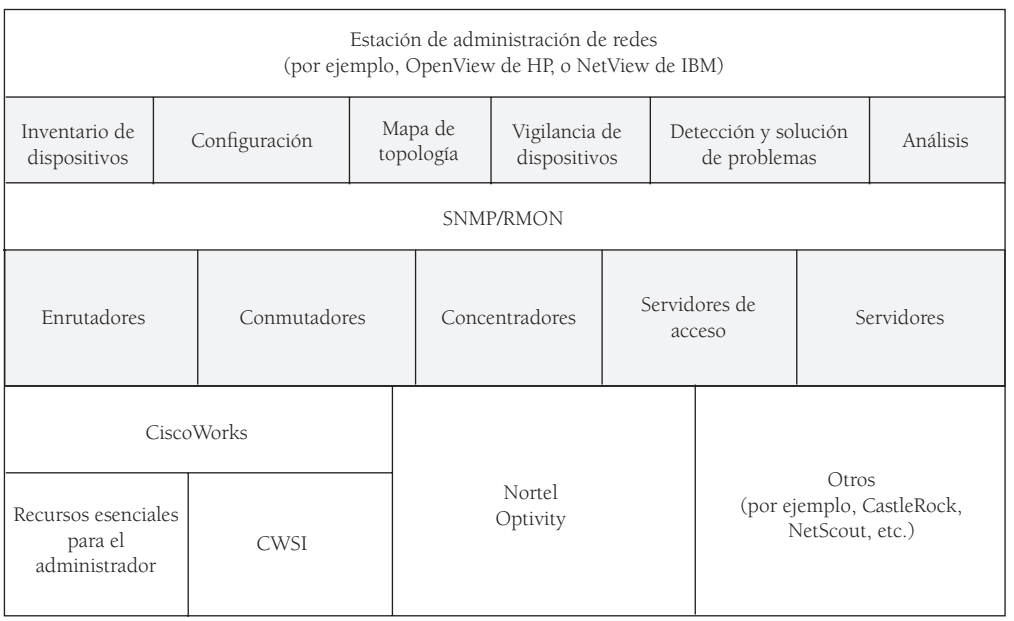


Sistemas de administración de redes

Durante la década pasada, una segunda generación de herramientas de administración surgió con la forma de sistemas de administración de redes. Esas herramientas se concentraban en la infraestructura de red en lugar del centro de datos. Estas herramientas usan las redes que administran como plataforma para vigilar eventos y son controladas desde una consola a la que se le denomina Network Management Station (NMS, estación de administración de redes).

La NMS líder es OpenView de Hewlett-Packard (HP). Hay mucha historia sobre la manera en que HP terminó en esta envidiable posición. HP se había comprometido con Unix como su sistema operativo estratégico a mediados de la década de 1980 (años antes otros comercializadores de plataformas). (No le dé mucho crédito a HP; lo hicieron debido a la desesperación porque su sistema operativo de propietario de 16 bits se había quedado sin combustible.) Por esa época, UNIX e IP se habían vinculado de cerca en el mercado, principalmente porque IBM y otros comercializadores de sistemas grandes estaban impulsando sus esquemas de redes de propietario. Alrededor de 1990, HP hizo su movida estratégica, y OpenView se subió al vagón del Unix para convertirse en la herramienta de administración de redes predominante. Ahora hay más de 100 000 instalaciones de OpenView.

Al igual que con Unicenter, la clave para el éxito de OpenView es la capacidad de trabajar con dispositivos de varios fabricantes, pero HP tenía una ventaja del diseño integrada en la forma del entonces nuevo estándar de administración de redes IP llamado Simple Network Management Protocol (SNMP, protocolo simple de administración de redes). En lugar de tener que diseñar docenas de interfaces de propietario, HP pudo dejar que los comercializadores de equipo de redes diseñarán productos para el estándar SNMP. OpenView fue el primer producto de administración importante que implementó SNMP.



La diferencia definitiva entre las consolas de sistema y de red es el nivel en el que operan. Las herramientas de administración de sistema se concentran en los sistemas opera-

tivos, las transacciones, los archivos de datos y las bases de datos tal como se encuentran en los servidores, los controladores de almacenamiento y los discos. Las herramientas de administración de redes se concentran en paquetes y conexiones como se encuentran en los dispositivos de red, las interfaces y los vínculos de transmisión.

Las consolas de sistema y de red ahora están convergiendo en una sola clase de tecnología que alguien llamó herramientas de Enterprise System Management (ESM, administrasión de sistemas empresariales). La convergencia en ESM es inevitable porque la línea entre las redes y la computadora es borrosa y las empresas completan su cambio al área a las arquitecturas cliente servidor que mueven recursos del centro de datos hacia las topologías de interconexión.

El eje de este libro es la interconexión, así que cubriremos sólo los componentes de interconexión de ESM.

Herramientas de la administración de redes hoy en día

Se ha probado que es muy difícil administrar una interconexión usando una sola herramienta. El problema ha sido la incapacidad de reunir datos consistentes de los diversos dispositivos que existen en la mayor parte de las infraestructuras de tecnología de la información de la empresa. El problema no es en realidad de equipo antiguo en comparación con equipo nuevo, aunque es parte del punto. El principal conflicto es que casi todas los sistemas de administración de redes tienen implementaciones superficiales; en otras palabras, sólo pueden administrar pocos aspectos de la operación del dispositivo y dejar algunos dispositivos sin administrar.

Esto es así a pesar del hecho de que todos los fabricantes importantes de equipo de redes incluyen SNMP en sus sistemas operativos del dispositivo. La infraestructura base de SNMP está allí, pero los fabricantes de dispositivos apenas lo implementan por completo en sus productos. Hay varias razones para esto:

- ▼ **Consumo de recursos para la administración de redes** Cada ciclo de CPU que se gasta en reunir una medida o enviar un mensaje de SNMP, es un ciclo no usado para la carga de tráfico. La administración de red paga un costo en plataformas más lentas o hardware adicional.
- ■ **Soporte irregular de estándares por parte de los fabricantes** Sería muy caro para los fabricantes de dispositivos construir un cumplimiento completo en sus productos. El hardware de dispositivos necesitaría adecuarse para manejar el trabajo adicional de SNMP, elevando los precios en el proceso. Además, algunos fabricantes prefieren un poco de incompatibilidad con SNMP para llevar a los clientes hacia la estandarización en su línea de productos, porque la implementación de SNMT de un fabricante es más fácil que llevar los dispositivos de distintos fabricantes bajo el mismo régimen de administración.
- ■ **Mano de obra** Se necesita mucho tiempo y atención para que las empresas implementen y operen un sistema de administración de redes. Los equipos de administración tienen mucha presión para sólo mantener el ritmo con el crecimiento de la red. Pocos tienen la capacidad laboral para hacer un mayor uso de los sistemas basados en SNMT.
- ▲ **Clientes conscientes del precio** Los creyentes se fijan en los precios bajos. Los anaqueles relacionados con redes en las tiendas de tecnología de la información se

consideran como infraestructura, y los administradores exigen precios accesibles. El enfoque incesante en llevar hacia abajo el costo por puerto parece bueno en el papel, pero incurre en costos ocultos en la forma de activos mal utilizados.

Por esto, la mayor parte de las implementaciones de FNMP reúnen sólo información de alto nivel. Se vigilan menos procesos (llamados objetos), las muestras son más pequeñas, los ciclos de almacenamiento son menos frecuentes, etcétera.

A menudo, aunque una empresa *sí* quisiera más controles de administración de red, los puntos ciegos aún se crean a partir de dispositivos que no cumplen con los estándares. Los puntos ciegos ocurren cuando una directiva no puede imponerse en parte de una red debido a que un dispositivo no la soporta. Los puntos ciegos a menudo ocurren en las puertas de entrada de la espina dorsal, sobre todo para espinas dorsales conmutadas. Imagine el escenario descrito en la figura 13-2. La parte de la topología en la parte inferior ha implementado una directiva para administrar el uso del tráfico entre un par de hosts que se comunican entre sí. Pero el conmutador de en medio no está configurado para vigilar esto, lo que deja que la directiva SNVP quede sin imponerse más allá del conmutador.

La IETF (Internet Engineering Task Force) es responsable del estándar SRMP y tiene un duro trabajo. La implementación de cualquier estándar requiere aceptación coordinada de fabricantes y usuarios. Esto es difícil de impulsar, porque los fabricantes están ansiosos por la aceptación del mercado y la pérdida potencial de ventajas competitivas. Lo que es comprensible, entonces, es que el establecimiento de estándares siempre resulte en un proceso lleno de trucos. Pero se ha probado que el objetivo de una consola NMS integrada es particularmente elusivo por estas razones:

- ▼ **Dependencia del hardware** Cualquier estándar de computadora debe tratar con varias arquitecturas usadas por CPU, buses, interfaces de dispositivo, unidades de disco, etcétera. Esto complica el proceso de establecimiento de estándares y lo hace más caro para que los fabricantes lo cumplan. El problema aumenta debido al ámbito de la industria de la interconexión de usar la mayor cantidad posible de partes diferentes en sus líneas de productos. ¿Recuerda todas las arquitecturas diferentes de CPU que se encuentran en la línea de enrutadores de Cisco?
- ■ **Tecnología convergente** Hasta hace poco, las telecomunicaciones, el uso de red de datos y la computación se veían como industrias separadas y distintas. Cada una tenía sus propios cuerpos estándares y otros elementos de la industria. Pero hoy en día, todo este equipo ha caído bajo la tutela de los administradores de red. Esto ha aumentado el alcance de los estándares y unido diferentes campos de la ingeniería, lo que crea entornos cada vez más complejos para los administradores de red.
- ▲ **Cantidad enorme de tecnologías** Los avances incansables de la tecnología en todos los sectores de la computación (telecomunicaciones, sistemas operativos, CPU, cableado, etcétera) han presentado al IETF un blanco en constante movimiento, y un fabricante que ha obtenido una ventaja bien ganada suele ser renuente a seguir los estándares y facilitarle la vida a los competidores.

El progreso ha sido lento. Pero la falta de administración integrada no ha impedido el crecimiento explosivo en el tamaño y uso de las redes. Para adecuarse a este conflicto, los equipos de administración usan varios productos para dar seguimiento a partes diferentes de sus interconexiones. Casi todas las empresas grandes tienen un ESM, pero lo aumentan con herramientas dedicadas a administrar partes críticas de las interconexiones. En la figura 13-3

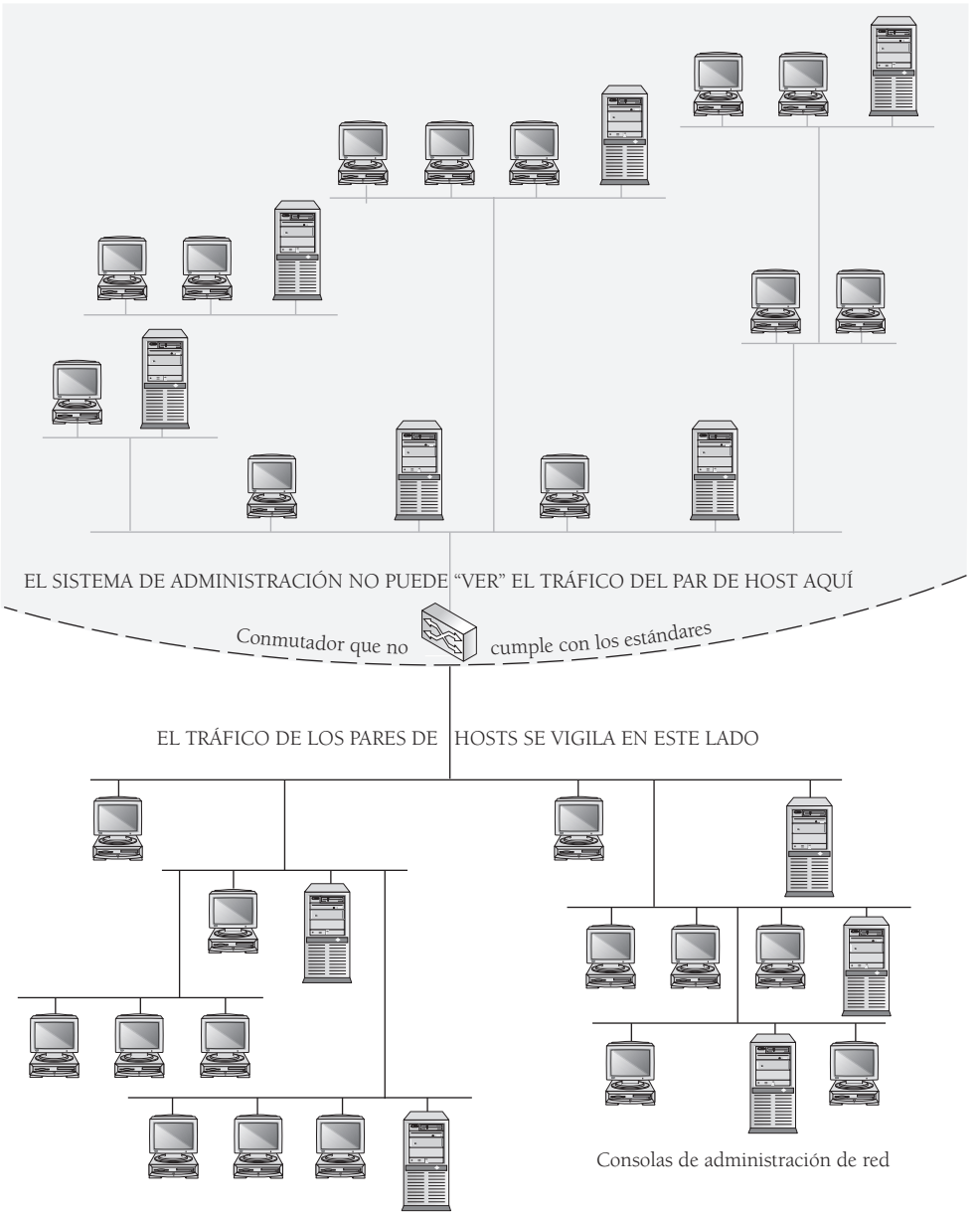


Figura 13-2. La administración parcial de SNMP origina puntos ciegos en la administración de redes.

se ilustra un escenario típico, con OpenView usado en vigilar la red general y herramientas específicas del fabricante para administrar los activos críticos.

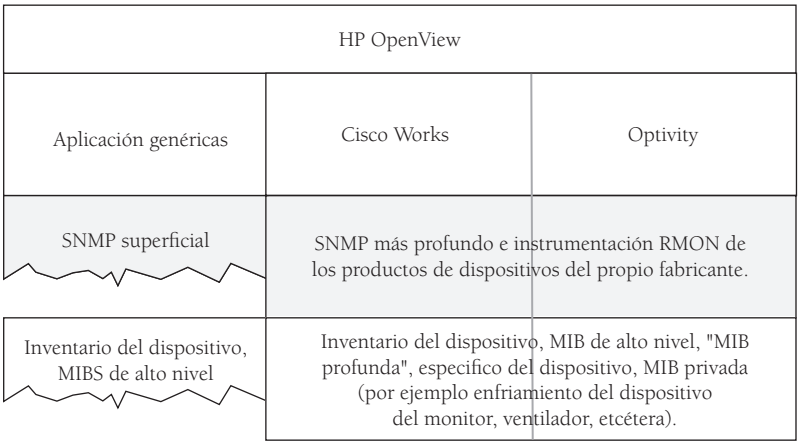


Figura 13-3. Casi todos los equipos de red usan varias herramientas para administrar sus redes.

La herramienta más importante que es específica del fabricante es CiscoWorks, con funcionalidad lo suficientemente amplia como para considerarse un ex ESM por sí solo (pero sólo mientras esté corriendo estrictamente equipo de Cisco) por eso, CiscoWorks suele incluirse en una suite de ESM como OpenView o NetView.

NOTA Los estándares de administración no sólo son un problema en las interconexiones. Un grupo de la industria llamada la Distributed Management Task Force (DMTF) ha tratado durante años de implementar un estándar llamado Desktop Management Interface (DMI, interfaces de administración de escritorio). El propósito de DMI, orientados a las PC distribuidas y servidores pequeños, es dejar que las consolas vigilen el inventario (discos, unidades de disco, versiones de BIOS, configuraciones de memoria, etcétera) y realicen actualizaciones remotas. Los productos DMI 2.0 incluyen Insight Manager de Compaq, Universal Management Agent de IBM, LANDesk de Intel, TopTools de HP y otros. El problema es que estos productos sólo trabajan con plataformas de su propio fabricante. Microsoft ha entrado con un estándar abierto llamado WBEM (Web-Based Enterprise Management, administración de empresas con base en Web), que se encuentra ahora bajo los auspicios de la DMTF. Intel está trabajando en un estándar complementario en el nivel de hardware llamado WfM (Wired for Management, conectado para administración). Por ahora, debe restringir el número de líneas de producto de comercializadores o usar herramientas individuales para administrar cada una de ellas. ¿Le suena familiar?

Tendencias en la adminsitración de sistemas empresariales

Las herramientas ESM han sido criticadas porque dificultan la implementación, requieren mucha mano de obra, son caras, lentas e inefectivas. Cuestan más de 250 000 dólares y se necesita por lo menos una cantidad similar para implementarlas. En cuanto hardware de administración especializado, RMON prueba que puede costar más de 10 000 dólares cada

uno. Los gastos han dejado a las interconexiones pequeñas y medianas depender de varias herramientas, y cada una suele ser específica de los principales fabricantes de equipo usados en la configuración. Un segundo resultado es que se monitorean menos cosas, lo que disminuye de manera pro activa la administración de las redes.

El mercado para herramientas de todos modos es grande porque el potencial para ahorrar a partir de herramientas NMS es enorme. Algunos estiman que durante un ciclo de vida típico de una infraestructura de tecnología de información, el 75% o más de todos los costos se gastan en operaciones. Hay un doble beneficio en permitir que el personal de administración de redes sea más productiva y obtengan mejores resultados en el ancho de banda disponible. Las herramientas en la NMS, ayudan a las empresas a reducir costos e impulsar los servicios al mismo tiempo.

Ahora hay muchas herramientas importantes de NMF. Además de OpenView, otras notables son Tivoli NetView de IBM (IBM adquirio Tivoli Systems hace varios años), CASpectrum, Enterprise Network Management Portfolio de Nortel Networks y OpenMaster de Evidian. Microsoft entró a la jugada con la presentación de Microsoft Management Console (MMC, consola de administración de Microsoft) en su versión de Windows 2000. Aún en expansión, MMC es una interfaz de administración clave en Windows Server 2003. No sólo se usa para herramientas de administración de Microsoft . Otros vendedores han creado sus propios complementos para la MMC también. En la figura 13-4 se presenta un cuadro de la manera en que se interrelacionan las diferentes herramientas de administración.

El reparto de contendientes viene de tres fuentes: fabricantes de plataformas de cómputo, como HP e IBM; fabricantes de dispositivos de red, como Cisco y Nortel Networks; y

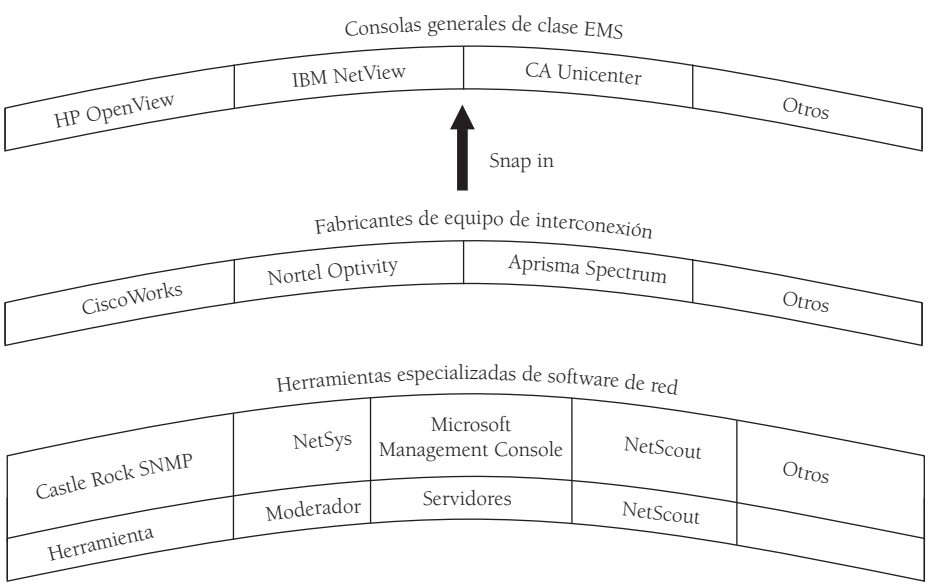


Figura 13-4. Hay varias herramientas de administración de redes y aplicaciones a disposición de los administradores de redes.

compañías de software en la forma de Microsoft, Castle Rock y otros. Quien prevalezca dirá que es lo más importante: el cable, el escritorio o él mainframe. Sin importar el comercializador, la tecnología NMS se encamina a cumplir estos objetivos:

- ▼ **Más cobertura** A medida que un control mayor de la administración se coloque en los dispositivos y los procesos de red, se requerirá hardware del dispositivo más rápido y más datos estarán disponibles.
- ■ **Simplicidad** A medida que las interconexiones han ganado popularidad entre las empresas pequeñas y medianas, es mayor la cantidad de personal no experto que está operando las redes.
- ■ **Automatización** A medida que las tecnologías de administración de redes mejoran, un mayor número de tareas de administración se están volviendo automatizadas para mejorar el aspecto de Quality of Service (QoS, calidad del servicio).
- ▲ **Indización pro activa** Una nueva camada de herramientas ayuda a aislar los problemas que surgen y a evitar problemas importantes de redes al tomar una acción correctiva temprana.

Casi todo el progreso en la computación es resultado directo o indirecto de los estándares de la industria. La interconexión anunció la era de la computación abierta con la ayuda de varios estándares: el modelo de referencia OSI y de varias capas, IP, Ethernet, Unix, HTTP, SQL y otros. Ahora es el momento de controlarlos con tecnología de administración integrada orientada por SNMP.

SNMP ES UNA PLATAFORMA DE ADMINISTRACIÓN COMÚN IP

Casi todos los conjuntos modernos de administración de interconexiones están construidos sobre el protocolo simple de administración de redes. Por tanto, antes de analizar las aplicaciones de administración de Cisco, un vistazo a esta tecnología de administración de redes es pertinente.

¿Qué es SNMP?

SNMP es un protocolo de TCP/IP construido con el propósito de servir como canal de comunicaciones para la operación de administración de interconexiones en la capa de aplicación de la pila IP. Aunque SNMP puede operarse directamente a través de la línea de comandos, casi siempre se usa mediante una aplicación de administración que emplea el canal de comunicaciones SNMP para monitorear y controlar las redes. Como se muestra en la figura 13-5, SNMP tiene dos componentes básicos: una estación de administración de red y agentes.

Los *agentes* son pequeños módulos de software, que reciden en dispositivos administrados, que pueden configurarse para reunir piezas específicas de información en operaciones de dispositivo. Casi toda la información consta de totales, como bits totales, paquetes totales, errores totales y cosas por el estilo. Los agentes pueden desplegarse en una gran cantidad de dispositivos, como:

- ▼ Enrutadores.
- ■ Conmutadores.

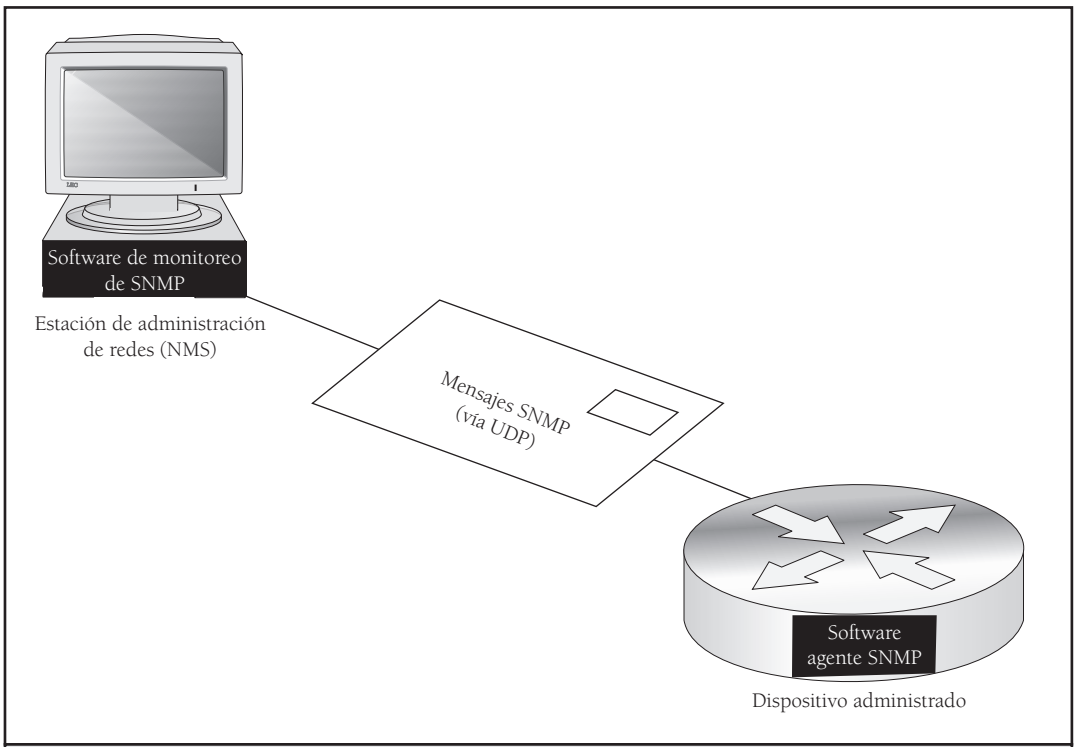


Figura 13-5. SNMP es un canal de comunicación para administración de redes.

- Servidores de acceso.
- Servidores (Windows, Unix, Linux, MVS, VMS, etcétera).
- Estaciones de trabajo (PC de Windows, Macs, Unix y escritorios de Linux).
- Impresoras.
- ▲ Sistemas de respaldo de suministro de energía eléctrica ininterrumpida.

La idea es colocar agentes en todos los dispositivos de red y administrar las cosas de acuerdo con la información de estado que se envía de regreso. Una pieza de equipo con un agente SNMP cargado se le denomina *dispositivo administrado* (también denominado *elemento de red*).

La NMS es el centro de control de la interconexión. Por lo general, sólo hay una NMS por cada sistema autónomo, aunque muchas interconexiones grandes usan más de una NMS (por lo general organizados en jerarquías). Casi todos las NMS de hoy en día se ejecutan en servidores Unix o Microsoft dedicados.

Encuestas SNMP y objetos administrados

SNMP es un protocolo de solicitud y respuesta muy simple. Funciona al encuestar a la NMS periódicamente administrado en busca de información fresca. La frecuencia con la que se encuestan depende de la opción de configuración, pero suele aplicarse una vez cada varios minutos más o menos. Hay tres tipos de encuestas:

- ▼ **Encuestas de monitor** Para revisar que los dispositivos estén disponibles y desencadenar una alarma cuando no lo estén.
- ■ **Encuestas de umbral** Para detectar cuando las condiciones se desvían de un número de línea base en un porcentaje mayor del permitido (por lo general más o menos de 10 a 20%) y para notificar a la NMS para su revisión.
- ▲ **Encuestas de rendimiento** Para medir el rendimiento continuo de la red en periodos largos y analizar los datos para conocer tendencias y patrones a largo plazo.

El agente responde a la encuesta al devolver un mensaje a la NMS. Puede hacer esto al capturar y almacenar información sobre temas que se han configurado para que se monitoreen. Estos temas suelen ser procesos relacionados con el flujo de los paquetes. Un proceso acerca del cual el agente reúne datos es llamado un objeto administrado. Un *objeto administrado* es una característica variable del dispositivo que se está administrando. El número total de conexiones UDP pude que abiertas en un dispositivo administrado, por ejemplo, podría ser un objeto administrado. Una sesión abierta de únete en una interfaz específica es una *instancia de objeto*, pero el número total de sesiones simultáneamente abiertas de un UDP en el dispositivo (digamos, un enrutador), es un objeto administrado. En la figura 13-6 se muestran conexiones UDP de ejemplo como objetos administrados e instancias.

Los objetos administrados suelen ser características operativas de dispositivos administrados. Los dispositivos administrados pueden estar en cualquier lugar de la topología (dispositivos de espina dorsal, servidores o sistemas finales) casi todos los objetos son piezas físicas, como una interfaz de red, pero un objeto administrado no es necesariamente una entidad física. Un objeto también podría ser una aplicación de software, una base de datos o alguna otra entidad lógica.

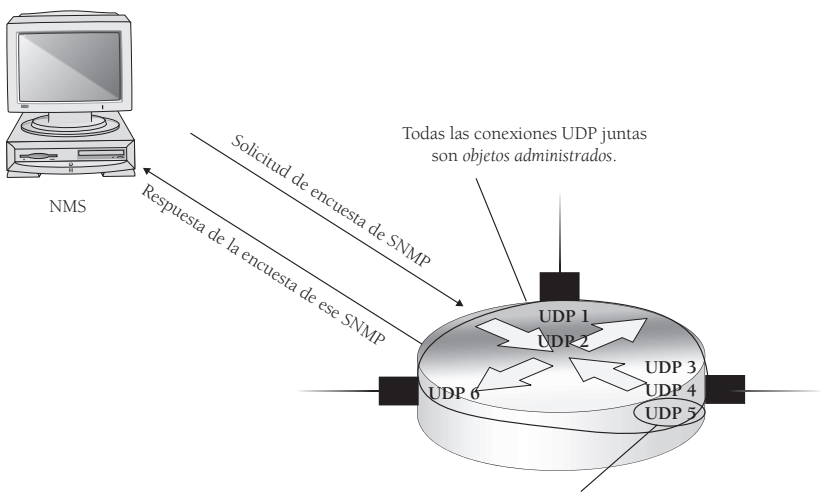


Figura 13-6. SNMP reúne información de dispositivos administrados.

La MIB

El agente almacena la información acerca de los objetos en registros especializados de datos llamados MIB (Management Information Bases, bases de información para la administración). La MIB es la parte de almacenamiento del software de agente SNMP. La información almacenada en las MIB se denominan *variables* (también llamados *atributos*). Las MIB suelen reunir información en la forma de totales para una variable durante un intervalo, como paquetes totales en cinco minutos. En el ejemplo de la figura 13-7 se muestran variables extraídas de instancias y procesadas a través de MIB administradas, y el objeto administrado (en este ejemplo, una cuenta de paquetes de Ethernet totales recorriendo una interfaz de enrutador). Una vez más la cuenta de paquetes de cada interfaz es una instancia de un objeto administrado; la cuenta para las tres interfaces es el objeto administrado.

Al reunir datos de varios objetos, la MIB permite que el agente envíe la información de NMS acerca de todo lo que se relaciona con el dispositivo que se está monitoreando.

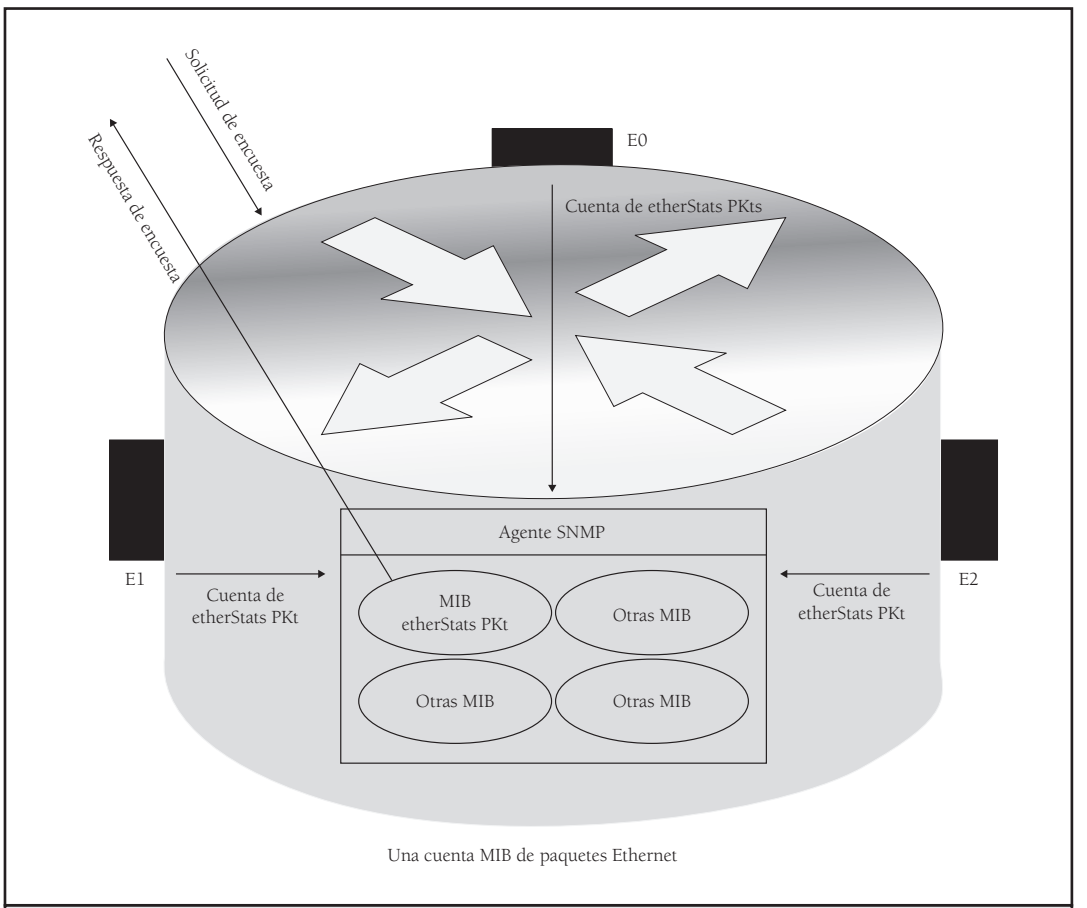


Figura 13-7. Las MIB son los bloques de construcción básicos de un sistema de administración SNMP.

Tipos de MIB

Las MIB están prefabricadas para realizar trabajos específicos. Las MIB suelen venir empaquetadas dentro del sistema operativo del dispositivo de red. Por ejemplo, el IOS viene empaquetado con MIB para la mayor parte de los trabajos de administración de redes.

Por lo general, a las MIB se les denomina usando una convención que indica la categoría relevante. A esto se le conoce como Object ID (OID, ID del objeto) de MIB.

Por ejemplo, un objeto MIB de Cisco que trata con una interfaz de red específica tendrá *if* en su nombre (de las letras *i* y *f* en interfaz). El objeto MIB ifInErrors monitorea los errores en paquetes entrantes de una interfaz; ifOutErrors monitorea los errores salientes, sysLocation aporta la ubicación de red de un dispositivo, etcétera. En la tabla 13-1 se muestran seis categorías de MIB básicas usadas en la mayor parte de los sistemas SNMP.

Categoría	Descripción y ejemplos
Configuración	Las MIB que reportan información de administración básica, como nombre del dispositivo, persona de contacto, ubicación del dispositivo y tiempo de conexión. Los objetos de configuración MIB son sysName, sysDescr, sysContact, sysLocation, sysUpTime, ifNumber, romID y otros.
Tasas de error de la interfaz	Las MIB que monitorean interfaces específicas. Los errores de paquete son una condición normal, pero la observación de sus tendencias indica la salud del dispositivo y ayuda a aislar fallas. Para las interfaces Thernet, use ifInErrors, ifOutErrors, locifCollisions, locIfInRunts, locIfInGiants, locIfCRC y otros. Para las interfases seriales, use locIfInFrame, locIfInAbort, locIfInIgnored, locIfResets, locIfRestarts y otros.
Ancho de banda	ICMP es un protocolo de capa 3 que informa sobre el procesamiento de paquetes IP. Se le conoce mejor por su comando **echo,** usado para verificar la presencia de otros dispositivos al hacer ping a ellos. Los Pings cronometrados se usan para determinar qué tan lejos se encuentra un dispositivo (de manera muy parecida a las películas de submarinos). SNMP envía mensajes de ping de entrada y salida para medir el ancho de banda disponible. Los objetos MIB de Cisco para esto son icmpInEchoes e icmpInEchoReps, además de icmpOutEchoes e icmpOutEchoReps. Hablando de manera general se trata sólo de mensajes SNMP no enviados como mensaje UDP.
Flujo de tráfico	La administración del rendimiento es en gran medida cuestión de medir el flujo del tráfico. Hay algunas MIB de Cisco para medir las tasas de tráfico, ya sea en bits por segundo o en paquetes por segundo: locIfInBitsSec, locIfOutBitsSec, locIfPktsSec y locIfOutPktsSec.
Dirección no alcanzable	El objeto para medir la frecuencia con que se pide a un enrutador que envíe mensajes a una dirección no alcanzable es icmpOutDesUnreachs.
Datos SNMP	Hay aún más objetos para medir cuánto tiempo tarda el enrutador en manejar mensajes SNMP. Entre los objetos se incluyen snmpInGetRequest y snmpOutGetRequests, snmpInGetResponses y snmpOutGetResponses, y otros.

Tabla 13-1. Objetos MIB de Cisco básicos de uso común en implementaciones SNMP.

Es posible reunir información sobre una sola instancia de objeto, llamada objeto *escalar*. Sin embargo, casi todos los objetos administrados están compuestos por varias instancias relacionadas. Esta práctica, llamada objetos *tubulares*, es la regla en la mayor parte de las MIB, porque es más eficiente de administrar de lo que sería posible para un solo punto de colección de datos. Como su nombre lo indica, una MIB tabular mantiene la información simple para almacenarla en filas y tablas.

NOTA La terminología de MIB puede ser confusa. Escuchará referencias a las MIB como si fueran un solo objeto MIB. Pero éste no es el caso. Por ejemplo, la MIB de Cisco no es una MIB; en realidad es la raíz de casi 400 objetos MIB privados de Cisco.

Lo que hace al SNMP independiente del equipo

No queremos hacer muy técnico este libro, pero debe comprender la manera en que los estándares SNMP se hacen a sí mismos independientes del equipo. En otras palabras, ¿cómo pueden ejecutarse en diferentes marcas de equipo, cada una con su propio sistema operativo de propietario?

El estándar SNMP requiere que cada objeto MIB tenga un ID de objeto y una sintaxis. Un ID de objeto identifica al objeto ante el sistema y le indica qué tipo de MIB usar y qué tipo de datos reúne el objeto. La sintaxis significa una especificación precisa que un equipo puede entender en un formato binario.

Para comprender el contenido de un campo, el IOS debe conocer si el campo contiene un número, texto, un contador u otro tipo de datos. A éstos se les denomina tipos de datos. Los *tipos de datos* especifican la sintaxis que se habrá de usar para un campo de datos. Un *campo* es una pieza de datos lógica, como un número de modelo o una lectura de temperatura. De la misma manera que un campo tiene su propio cuadro en una pantalla de entrada, tiene su propia posición en un archivo de computadora. Un archivo representa datos en binario (0 y 1) y un conjunto de posiciones binarias se reserva para cada campo dentro del archivo. Todos los campos deben declararse como algún tipo de datos u otro, o de otra manera la máquina no podrá procesar los datos contenidos allí.

Las arquitecturas de hardware de computadoras, sistemas operativos, lenguajes de programación y otros elementos ambientales especifican los tipos de datos que desean usar. Un tipo de datos representa la capa donde el software se une con el hardware. Le indica a la máquina qué sintaxis usar para interpretar el contenido de un campo. Una sintaxis diferente se usa para números de punto flotante, números enteros, fechas, cadenas de textos y otros tipos de datos.

SNMP se hace asimismo independiente al declarar sus propios tipos de datos. Lo hace así en la forma del estándar Structure of Management Information (SMI, estructura de información de administración). SMI es un estándar dedicado a especificar una sintaxis independiente de la máquina para cada tipo de datos. Estos tipos de datos son independientes de la estructura de los datos y las técnicas de representación únicas para las arquitecturas particulares de computación. SMI especifica la sintaxis para tipos de datos como ID de objeto, contadores, filas, tablas, cadenas de octetos, direcciones de red y otros elementos SNMP.

Los comercializadores programan las MIB empleando un lenguaje de programación antiguo denominado ASN.1, creado sólo para la programación de tipos de datos. SMI ASN.1 (Abstract System Notation One, notación de sistema abstracto uno) es un estándar OSI de

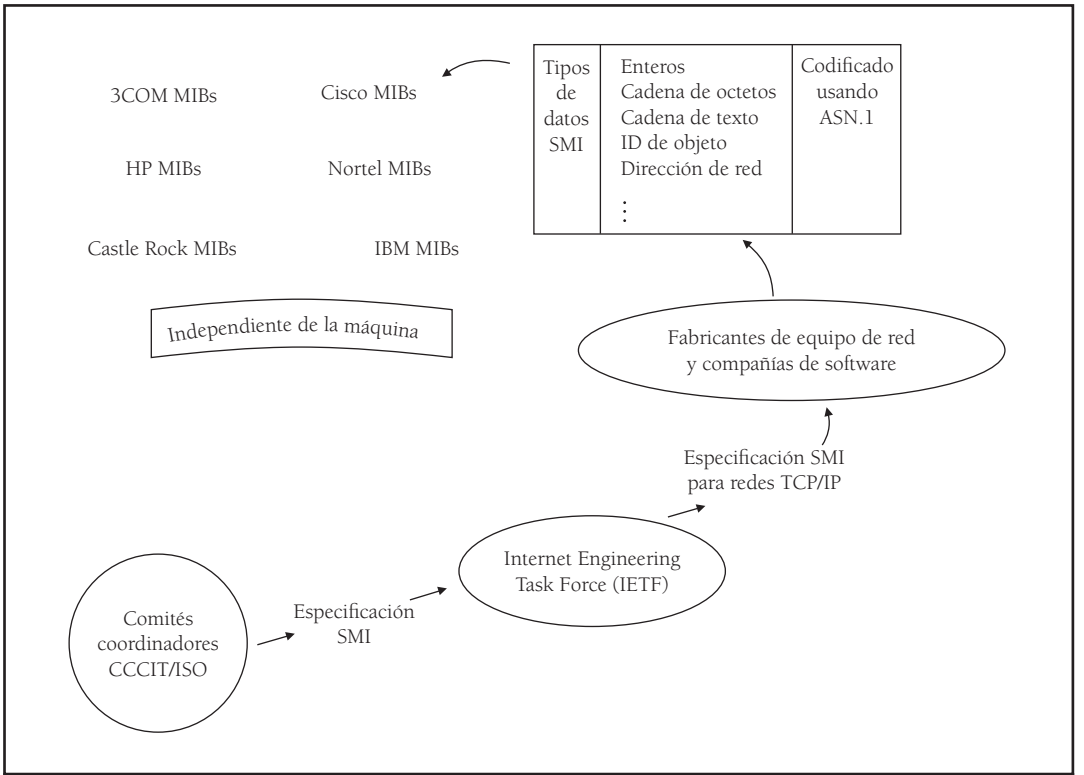


Figura 13-8. Las MIB están integradas usando tipos de datos SMI independientes de la máquina.

las mismas personas que nos trajeron el modelo de referencia de siete capas. En la figura 13-8 se muestra la manera en que los tipos de datos SMI universalizan la información de MIB.

SMI trata de dejar que los comercializadores unifiquen objetos MIB de escríbase una vez ejecútese donde sea. En otras palabras, alguien debe tener la capacidad de escribir una sola pieza de software de MIB (un contador de paquetes, por ejemplo) y el contador MIB debe tener la capacidad ejecutarse en cualquier dispositivo que soporte la definición de sintaxis SMI para un contador.

Los tipos de datos SMI son bloques de construcción SNMP en el nivel más bajo. Se usan para construir formatos de objetos MIB en una sintaxis que cualquier máquina pueda entender. A partir de allí, las instancias de objetos se miden y se envuelven en objetos administrados, que a su vez el agente SNMP reporta a la NMS. Así es como las NMS pueden operar entre arquitecturas de dispositivos dispares.

MIB estándares y privadas

El estándar MIB actual es MIB-II, que tiene casi 200 objetos estándar MIB. El estándar está implementado como una jerarquía que empieza de una raíz y continúa hacia las ramas de abajo desde la MIB de origen hasta la raíz MIB de Internet. En la figura 13-9, puede ver que cada rama está marcada con un nombre y un número (los números se usan para construir ID de objetos).

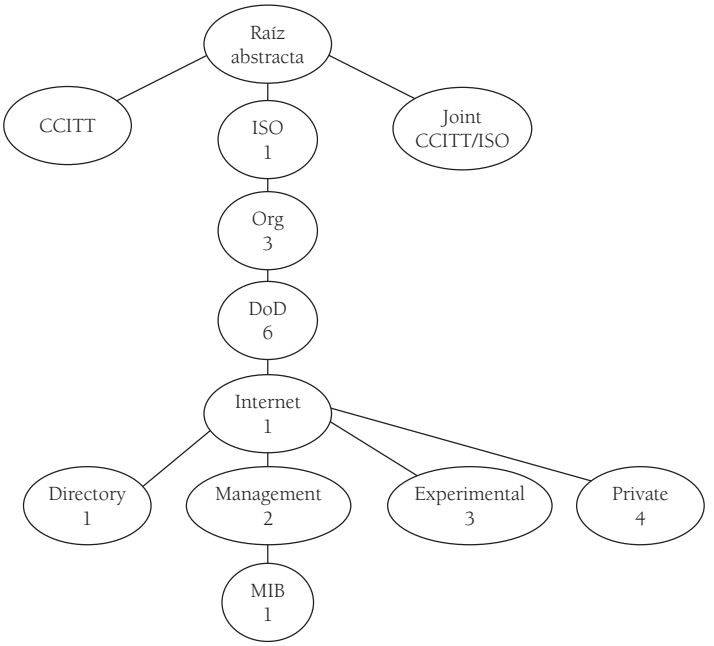


Figura 13-9. El linaje de la familia de Internet nos muestra el linaje estándar del MIB de Internet.

En la figura 13-9 también se muestran los jugadores en la historia de Internet. ISO es la International Standards Organization, y DoD es el departamento de la Defensa de Estados Unidos (que lo empezó todo con ARPANET). CCITT es el Consultative Committee for International Telegraph and Telephone. El CCITT es sólo un primo distante de Internet, el cual maneja la telefonía y otros estándares de comunicación. El CCITT ahora es conocido como el ITU-T (el sector de estandarización en telecomunicaciones del International Telecommunications Union), pero aún verá el acrónimo CCITT unido a docenas de estándares.

Como son más amables con el usuario, las cadenas de texto se usan usualmente para describir objetos MIB en directorios. Los ID de objeto son principalmente usados por el software para crear representaciones compactas, codificadas de nombres.

El trabajo con la estructura de árbol de la figura 13-9, el ID de objeto de la raíz de Internet es 1.3.6.1., llamado iso.org.dod.internet. Las dos ramas que parten de la raíz de Internet son las MIB de administración y privadas. La MIB estándar de la industria recorre la rama de administración para convertirse en iso.org.dod.internet.mgmt.mib con el ID de objeto 1.3.6.1.2.1. Las MIB privadas se vuelven iso.org.dod.internet.private y 1.3.6.1.4. La MIB privada de Cisco está representada como iso.org.dod.internet.private.enterprise.cisco, o el ID de objeto 1.3.6.1.4.1.9.

Los comercializadores pueden construir MIB privadas al extender las ramas del estándar. De esta manera, pueden personalizar MIB para que se adecue mejor a sus necesidades

particulares. En la figura 13-10 (la jerarquía de la MIB privada de Cisco) muestra la manera en que las MIB privadas se extienden a partir de la MIB de Internet de estándar.

Muchos de los grupos de objetos dentro de los subgrupos Management, Temporary Variables y Local Variables de Cisco miden la tecnología de propietario de Cisco. Por ejemplo, el grupo Cisco Environmental Monitor del subgrupo Cisco Management (ID de objeto 1.3.6.1.4.1.9.9) busca cosas como la temperatura de operación dentro del dispositivo. Ese tipo de información es el elemento a "profundidad" del que estamos hablando en relación con las aplicaciones de administración con los que otros fabricantes han tenido problemas.

Otra cosa importante que se debe observar en la figura 13-10 es el soporte para los protocolos de escritorio heredados. Novel Netware IPX, VINES, AppleTalk, DECnet e incluso redes Xerox XNS pueden administrarse con MIB de Cisco. Éstos son heredados porque la especificación LAN de IP parece ser la dominante en el mercado, pero las otras aún están en uso y por tanto son importantes para sus clientes.

Encuesta de grupos y agregación de datos

Las MIB suelen colocarse frecuentemente en grupos de encuestas para facilitar la recolección de datos SNMP. Un *grupo de encuestas* es un conjunto de objetos administrados con relación lógica que son reportados y analizados como una entidad coherente. Por ejemplo, en la figura 13-11 se muestran los grupos de encuestas de tres diferentes clases de equipo en una interconexión: los conmutadores de espina dorsal, enrutadores y servidores de aplicaciones. Las

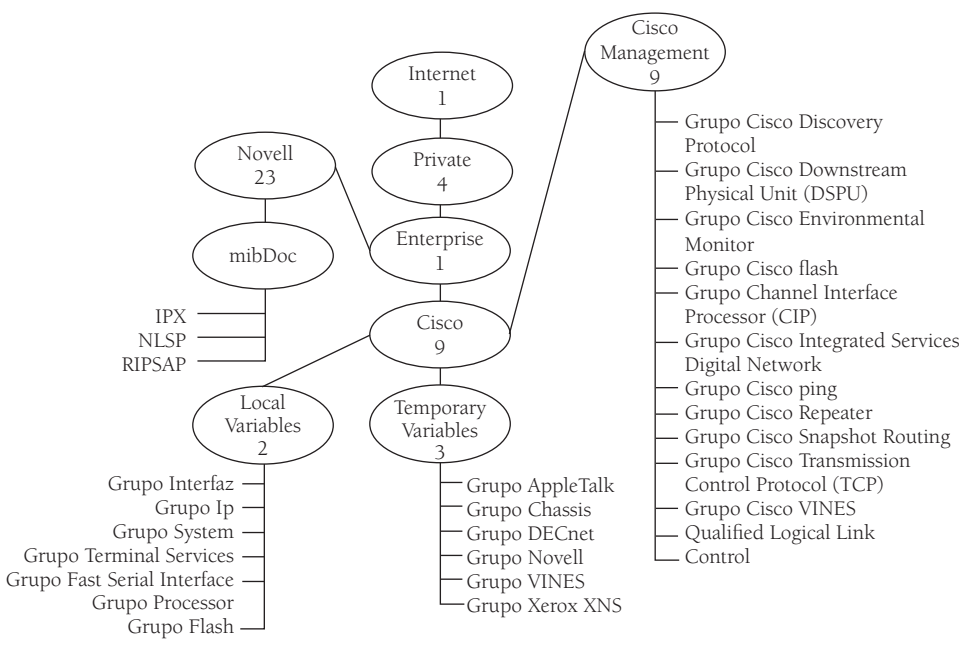


Figura 13-10. Las ramas de la jerarquía privada de Cisco en cuatro subgrupos.

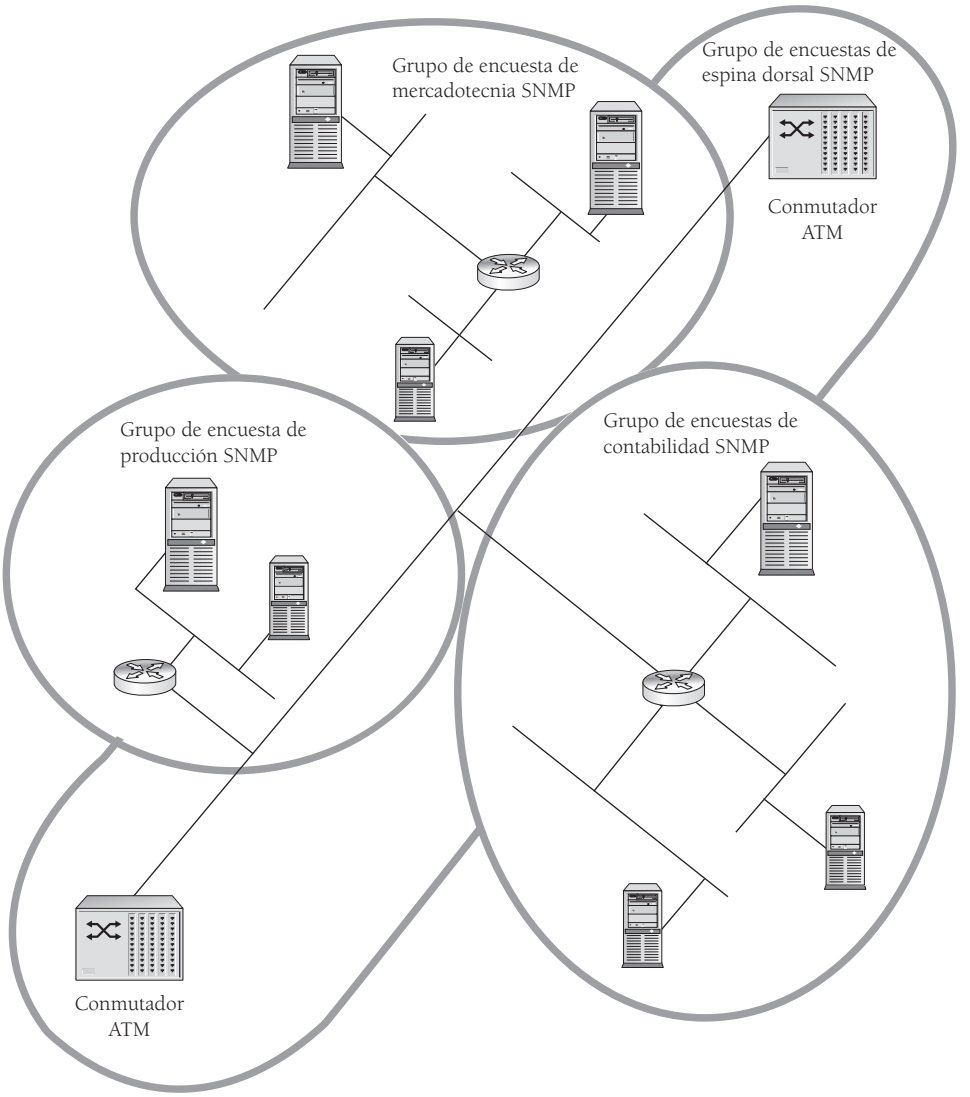


Figura 13-11. La encuesta de grupos se usa para ayudar a hacer que los datos SNMP sean más manejables.

diferentes variables de MIB es probable que estén reunidas para cada tipo, de modo que cada uno obtiene su propio grupo de encuestas. De esta manera, la información de administración con relación lógica se compila y almacena en una base de datos de SNMP bajo este grupo.

La creación de grupos simplifica el trabajo del administrador. En el ejemplo de la figura 13-11, pueden establecerse umbrales para satisfacer las tolerancias apropiadas para cada grupo. Por ejemplo, es probable que un equipo de red establezca variables de alarma más

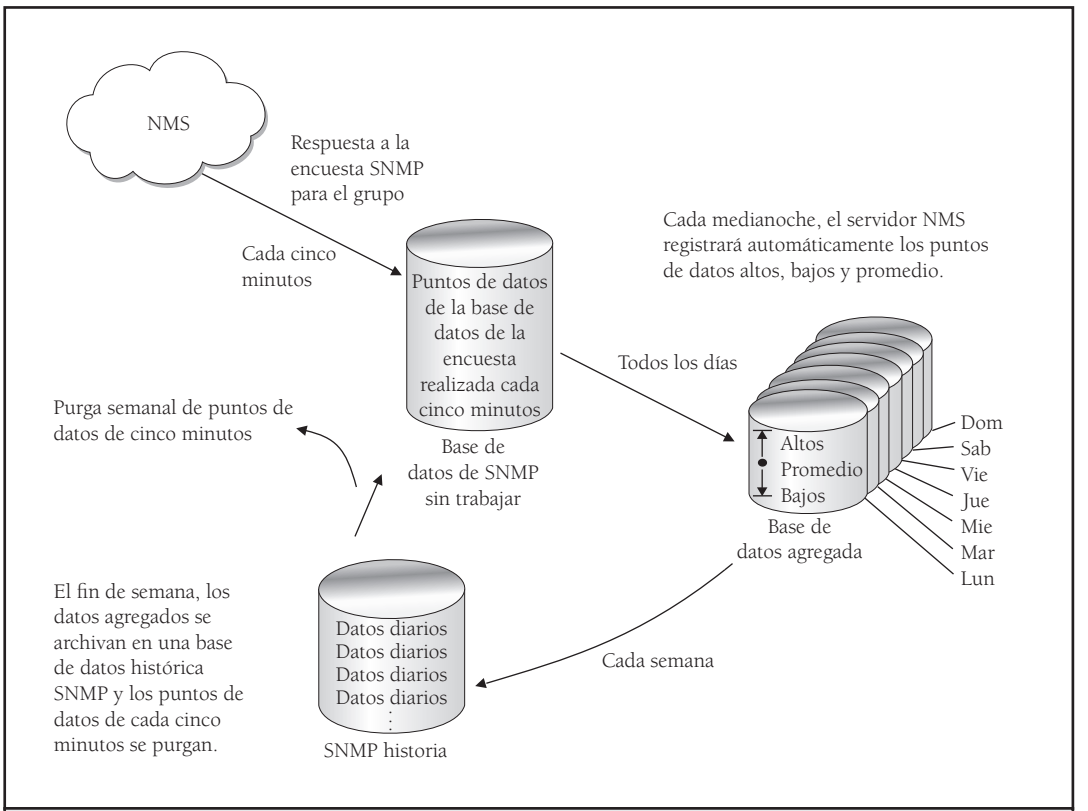


Figura 13-12. La agregación de datos resume los datos mientras preserva su integridad.

sensibles para los conmutadores de espina dorsal, debido a que el problema con ellos podría hacer que deje de funcionar toda la red. La encuesta de MIB similares en masa, simplifica las operaciones SNMP y ayuda a asegurar que los datos sean consistentes, confiables y más fáciles de asimilar.

Los grupos también facilitan la limitación de la cantidad de información que se almacena en la base de datos NMS. SNMP podría construir montañas de datos en cada dispositivo de una red, pero al hacerlo no sería práctico ni valdría la pena. El almacenamiento de información sobre grupos MIB relacionados facilita el movimiento de datos sin trabajar por un ciclo de agregación y purga. En la figura 13-12 se muestra un escenario típico, en que las variables MIB de un grupo son encuestadas y almacenadas en la base de datos NMS cada cinco minutos. Cada medianoche, los datos se agregan en mínimos, máximos y promedios para cada hora y se almacenan en otra base de datos. Los puntos de datos se purgan de la base de datos cada semana, dejando sólo los datos agregados.

El ciclo recolección, agregación y purga, tiene varios beneficios. Mantiene el espacio de disco abierto en el servidor NMS para almacenar nuevas MIB y mantiene integridad estadística del registro de datos. Al mismo tiempo, también mantiene una imagen consistentemente actualizada de las operaciones de red.

Comandos SNMP

El *simple* de protocolo simple de administración de red, viene del hecho de que el protocolo tiene sólo seis comandos raíces. Se usan para establecer parámetros SNMP dentro del archivo config del dispositivo. He aquí los comandos SNMP de raíz:

- **Get** Lo usa NMS para recuperar instancias de objetos de un agente.
- **GetNext** Se usa para recuperar instancias de objeto subsiguientes después de la primera instancia.
- **GetBulk** Esta operación recupera todas las instancias en un objeto administrado (reemplazando la necesidad de operaciones Get Next iterativas).
- **Set** Se usa para establecer valores para instancias de objetos dentro de un agente (como un umbral).
- **Trap** Se usa para instruir a un agente que notifique de manera unilateral a la NMS de un evento (sin ser encuestados).
- **Inform** Este comando instruye a una NMS que rendirija la información atrapada de uno o más NMS adicionales.

NOTA Casi todo el tiempo, las computadoras usan los comandos SNMP en lugar de que lo hagan las personas directamente. Por ejemplo, si un administrador ingresa la ubicación de un enrutador en una pantalla de inventario en la consola Essentials, se lanza un proceso desde Essentials que cambia el **set snmp location** en el IOS dentro de ese enrutador, y el valor de la MIB se actualiza de acuerdo con ello.

Los dos comandos básicos SNMP son **get** y **set**. El comando **set** se usa para establecer parámetros administrados en objetos administrados. Cuando utiliza un comando SNMP SEt, configura el dispositivo de red con el valor correspondiente (como lo definió la MIB). Así, por ejemplo, si el administrador ingresa la ubicación de un enrutador en una pantalla de inventario de una estación de administración SNMP, esto, a cambio, usa los comandos SNMP set para establecer este valor de ubicación en el enrutador.

Por el contrario, el comando **get** se usa para buscar variables almacenadas de los agentes y traerlos de regreso al NMS.

SNMP necesita ser simple para lograr que obtenga soporte por parte de arquitecturas dispares. Esto es un requisito práctico para la interoperabilidad de SNMP.

Umbrales

Un *umbral* define un valor aceptable o un rango de valores para una variable SNMP en particular. Cuando una variable excede una directiva, se dice que ha tenido lugar un *evento*. Un evento no es necesariamente una situación de esto o lo otro, como apagar un conmutador. Los eventos suelen ser irregularidades de la operación sobre la que el equipo de red no querrá saber antes de que el servicio sea afectado. Por ejemplo, tal vez un administrador de red establezca una directiva para el número de errores de paquete que ocurren en una interfaz para poder dirigir el tráfico alrededor de cuellos de botella que surgen. Los umbrales pueden establecerse como un techo o como un rango con límites superior e inferior. Los dos tipos de umbrales se describen en la figura 13-13.

Las partes compartidas de la figura 13-13 se denominan *eventos de umbral*. En otras palabras, un evento es cuando algo ha tenido lugar en violación de la directiva establecida. Un

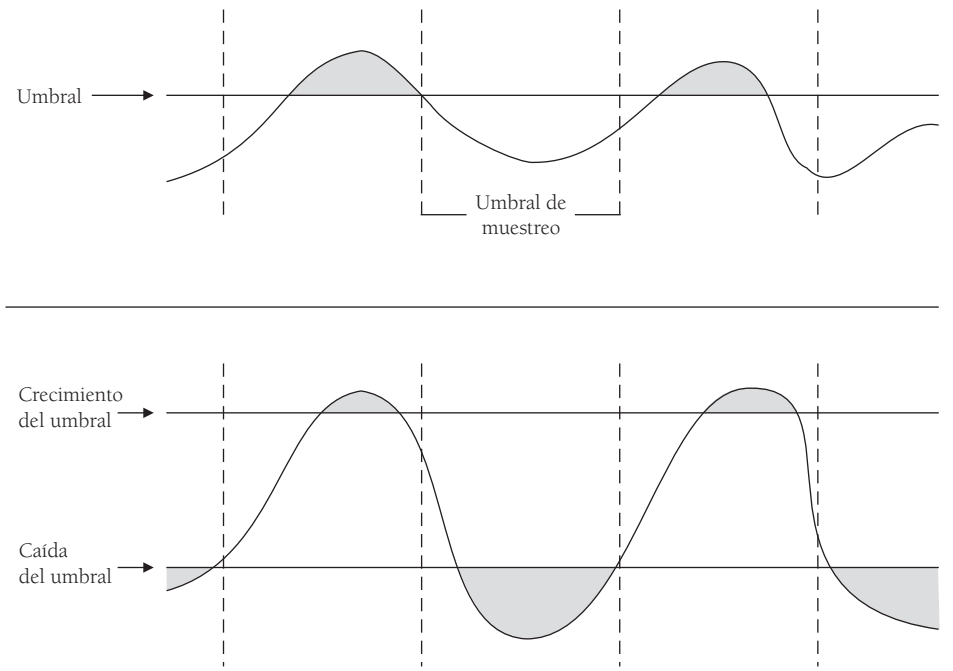


Figura 13-13. Los umbrales establecen un rango de operación normal para un objeto administrado.

intervalo de *muestreo* es el periodo en que cada estadística se compila. Por ejemplo, un objeto MIB puede almacenar el número local de errores de paquete que tienen lugar durante cada periodo de cinco minutos. Los intervalos deben ser lo suficientemente largos para reunir una muestra representativa, pero lo suficientemente cortos para capturar eventos antes de que puedan afectar de manera sustancial el rendimiento de la red.

Eventos y trampas

Cuando ocurre un evento, el administrador de red puede especificar la manera en que el agente SNMP debe responder. El evento puede registrarse o puede enviarse un mensaje de alarma a la NMS. Un mensaje de alerta SNMP es denominado *trampa*, y se le llama así porque captura (atrapa) el evento en el dispositivo. Para aclarar esto, una alarma es un tipo de mensaje de alerta. Una trampa contiene información acerca del evento. En la figura 13-14 se muestra el curso de los eventos que llevan al disparo de una alarma.

Las alarmas pueden tomar muchas formas. A medida son configuradas para mostrarse a sí mismas como un icono que parpadea en la consola de la NMS, pero podría hacer que se genere un ruido. Las redes que no tienen administradores presentes en la NMS todo el tiempo hacen que la trampa marque a un localizador o envíe un correo electrónico con prioridad para alertar a la persona responsable de esta tarea en ese tiempo.

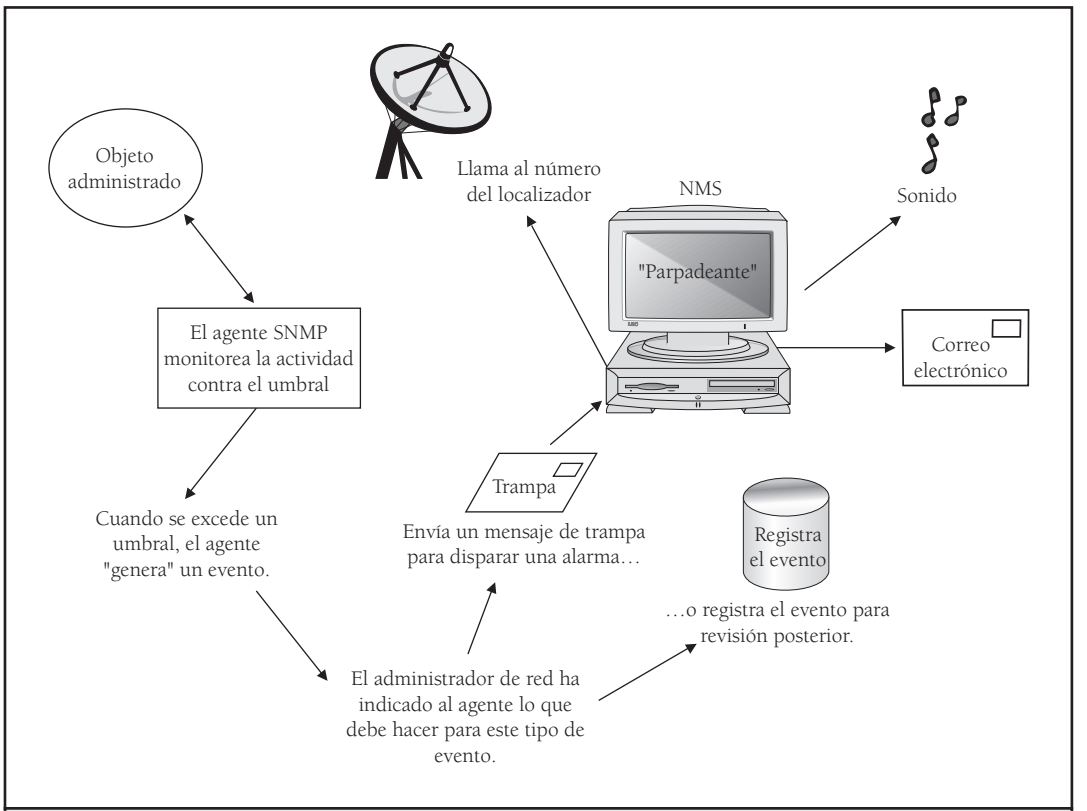


Figura 13-14. Una trampa SNMP reporta pro activamente un evento al NMS.

Las trampas no sólo se usan para enviar alarmas. A medida que crece el tamaño de una interconexión, el tráfico excedente del SNMP aumentará junto con ello. Los administradores de red pueden reducir la sobrecarga de SNMP al aumentar la frecuencia de la encuesta, pero al hacer esto hace que la NMS responda con menos frecuencia a los problemas de red que surgen. Una mejor manera de limitar la sobrecarga del SNMP es usar trampas. Dado que son mensajes no solicitados en lugar de respuestas a encuestas de SNMP, las trampas consumen una cantidad insignificante de ancho de banda.

El siguiente fragmento de código es de un archivo config del enrutador de Cisco. Éste muestra la configuración del SNMP hecha por el dispositivo. RO y RW son cadenas comunitarias de sólo lectura y de lectura-escritura, respectivamente, que hacen que el dispositivo sea un miembro de un grupo de administración determinado.

```
MyRouter(config)#snmp-server community yellow RO
MyRouter(config)#snmp-server community blue RW
MyRouter(config)#snmp-server enable traps snmp
MyRouter(config)#snmp-server enable traps isdn call-information
MyRouter(config)#snmp-server enable traps config
MyRouter(config)#snmp-server enable traps bgp
MyRouter(config)#snmp-server enable traps frame-relay
```

```
MyRouter(config)#snmp-server enable traps rtr
MyRouter(config)#snmp-server host 10.1.1.13 traps vpi
```

Varias trampas de SNMP están habilitadas en este archivo. Esto indica al agente de SNMP en el dispositivo que envíe mensajes de trampa si cualquier cosa cambia. La última línea da la dirección IP del NMS para que el agente sepa a dónde enviar los mensajes atrapados.

RMON: sondas de hardware para redes conmutadas

RMON (*remote monitoring, monitor remoto*) es un estándar de administración separado pero relacionando que complementa a SNMP. RMON es similar a SNMP de varias maneras: es un estándar abierto administrado por la IETF; usa tipos de datos SMI y el formato raíz de MIB; y reúne datos de dispositivo y lo reporta a un NMS. Pero RMON difiere del SNMP normal en estas maneras fundamentales:

- ▼ RMON está basada en instrumentos, porque usa hardware especializado para operar.
- ■ RMON envía activamente datos en lugar de esperar a que sean encuestados. Al hacerlo eficiente para ancho de banda y con más capacidad de respuesta a eventos de red.
- ▲ RMON permite que se reúnan datos mucho más detallados.

La instrumentación de RMON es más poderosa, pero más costosa. Consecuentemente, las sondas de RMON vienen a colocarse en vínculos críticos, como espinas dorsales de red y servidores importantes.

RMON y redes conmutadas

El movimiento hacia la administración de redes basada en RMON está vinculado muy de cerca con el crecimiento de las redes vinculadas. Mientras que la conmutación de LAN está a la alza como la manera de mejorar el desempeño de las redes, plantea problemas especiales para los métodos de administración convencionales del SNMP. En una red formada utilizando concentradores, un analizador LAN tiene visibilidad completa porque el medio es compartido por todos los nodos. Pero una LAN conmutada no es un medio compartido, de modo que para mantener el mismo nivel de visibilidad, el analizador tendría que colocarse en cada puerto conmutado. La solución consiste en incorporar el analizador (o por lo menos la parte del sensor de él), directamente en el hardware del conmutador. Eso es una sonda RMON. En la figura 13-15 se muestra una red conmutada administrada con y sin RMON.

RMON se convirtió en el estándar en 1992 con el lanzamiento de RMON-1 para Ethernet. El estándar RMON-2, la versión actual, se completó en 1997. Mientras que MON-1 operaba sólo en las capas físicas y de vinculación de datos (capas 1 y 2) en el modelo de referencia OSI de siete capas, RMON-2 agrega la capacidad de recolectar datos en capas más elevadas, dándole más capacidad para la creación de informes. La capacidad de monitorear eventos de la capa superior ha sido un impulsor de la popularidad de RMON. Por ejemplo, RMON-2 puede informar lo que está sucediendo con el tráfico de IPX en oposición a IP en un segmento LAN de varios protocolos.

El RMON remplaza a los dispositivos de analizador de red costosos que deben conectarse físicamente al área aproximada de un problema de red. Las sondas RMON toman diferentes formas, dependiendo del tamaño y el tipo de dispositivo que habrá de vigilarse:

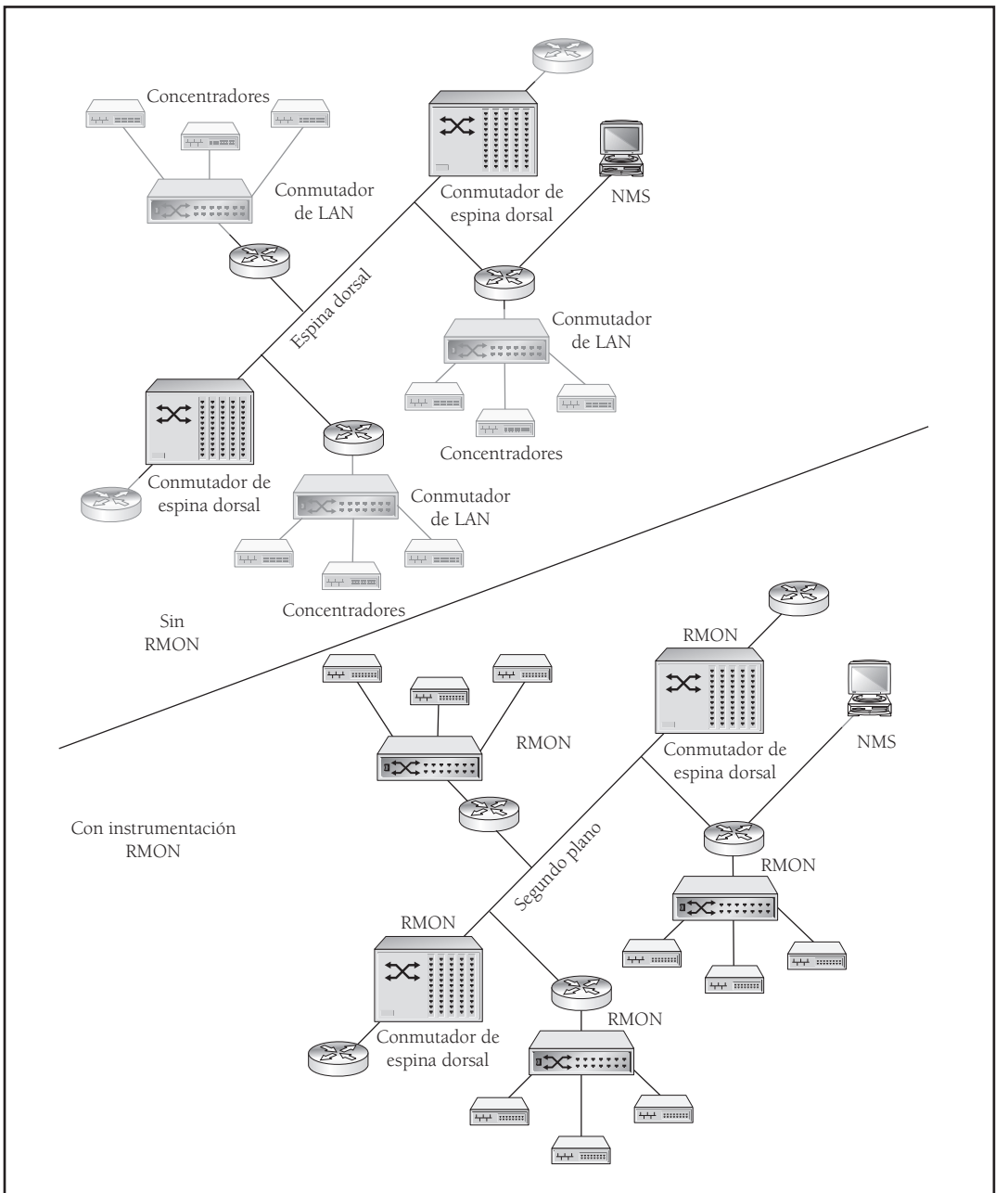


Figura 13-15. Las sondas RMON proporcionan visibilidad de administración entre las redes conmutadas.

- Una MIB de RMON que usa el hardware de dispositivo monitoreado (llamado *agente incrustado*).

- Un módulo de tarjeta especializado que se inserta en una ranura dentro del dispositivo monitoreado.
- Una sonda construida con un propósito específico, conectada externamente a uno o más dispositivos monitoreados.
- ▲ Una PC dedicada, conectada a uno o más dispositivos monitoreados.

Tener hardware especializado ubicado de manera remota con un dispositivo monitoreado presenta sus ventajas. Las sondas RMON pueden arrojar un conjunto mucho más rico de datos de medición de lo que lo haría un agente SNMP. El hardware dedicado se usa como censor en tiempo real que puede reunir y analizar datos para cada posible NMS.

Los nueve grupos del MIB de RMON

Otra ventaja de RMON es que disfruta su libertad como un estándar separado. La MIB raíz de RMON define nueve grupos especializados de MIB (y un grupo Token Ring). Los grupos permiten que RMON recolecte información de administración más detallada y fina de lo que sería utilizando SNMP. En La figura 13-16 se presenta una gráfica de las MIB de RMON.

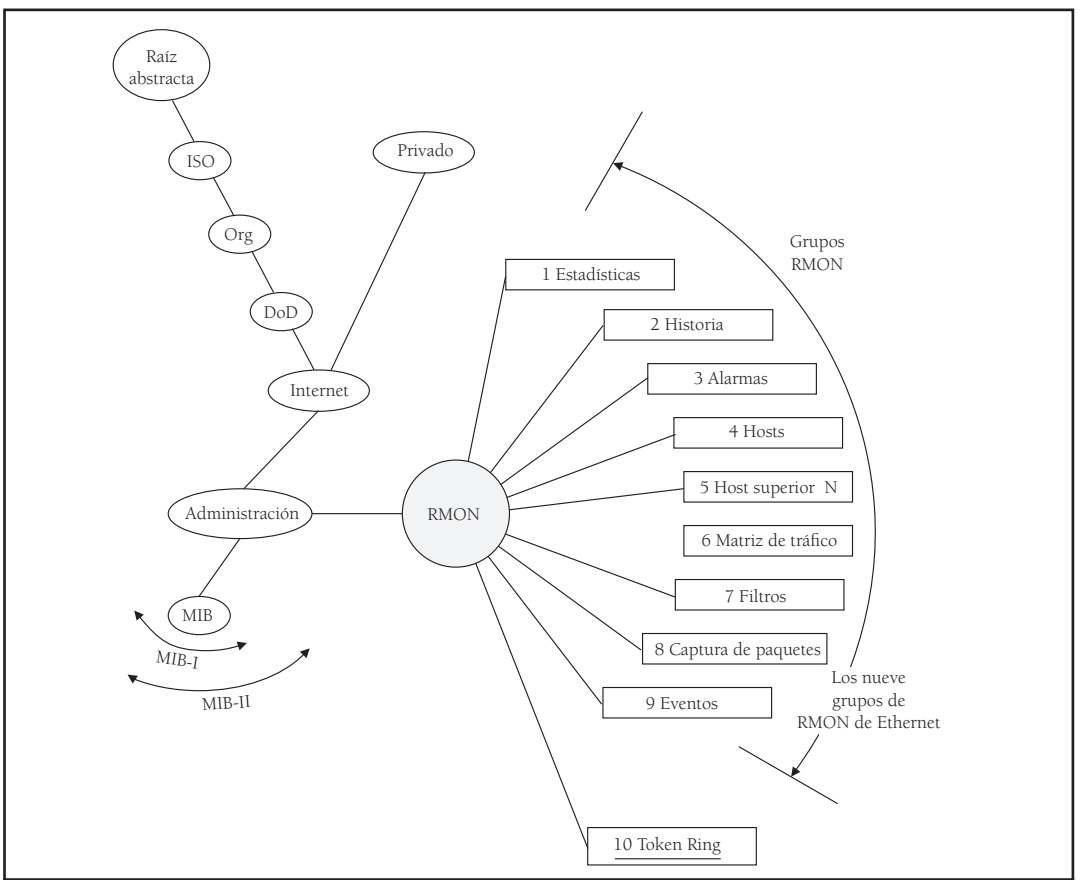


Figura 13-16. RMON almacena datos de administración de Ethernet en nueve grupos especializados.

RMON, como mínimo, viene con los grupos eventos y alarma. Muchos vienen con los cuatro grupos necesarios para la administración básica: eventos, alarmas, estadísticas e historia. Debido al costo del hardware y a las preocupaciones del tiempo de respuesta, los grupos que requieren muchos recursos para funcionar, como el grupo matriz de tráfico, se despliegan con poca frecuencia.

La alarma MIB de RMON es un mecanismo más poderoso para la administración de eventos que SNMP. Por ejemplo, como una MIB separada sólo para llevar registro de los eventos, RMON puede ajustarse para evitar el envío de demasiadas alarmas. Además, la MIB Matrix puede monitorear el tráfico basado en "conversación". En otras palabras, puede configurarse para monitorear las conexiones entre paredes de direcciones MAC y reportar lo que está sucediendo con cada conexión. Por ejemplo si una MIB matriz fue configurada para vigilar un vínculo costoso, digamos, entre Nueva York y Londres, y alguien está usándolo para jugar un juego de DOOM trasatlántico, la MIB puede ver eso y alertar al NMS que se está desperdiciando un valioso ancho de banda.

El problema con RMON es que es costoso. Requiere hardware adicional para almacenar y analizar paquetes en tiempo real y eso cuesta dinero. Por tanto, RMON sólo se está utilizando para administrar vínculos que son críticos para la misión o costosos.

Tendencias en la tecnología de administración de red

Los problemas de cumplimiento con SNMP han dejado a las nuevas versiones del estándar empantanado en luchas políticas. Además, el rápido desarrollo de herramientas poderosas basadas en RMON está empujando a la administración de red en una nueva dirección. La tecnología que apoya las aplicaciones de administración de redes muestra esta tendencia:

- ▼ Recolección de datos más poderosa (más información se reporta con mayor rapidez).
- ■ Administración más pro activa.
- ■ Soporte integral mejorado del hardware para la administración.
- ▲ Mejor seguridad para proteger las herramientas de administración.

La tendencia hacia una administración más intensiva de las interconexiones está enfrentando el mismo problema de siempre: cada mensaje de administración es un excedente que consume precioso ancho de banda. Este dilema es lo que está empujando la industria hacia RMON, porque esa tecnología captura mejor información y trabaja de manera local (en lugar de hacerlo a través de encuestas de NMS).

Las otras tendencias tienen que ver con hacer que los sistemas de administración sean más eficientes y proporcionen al SNMP una mejor seguridad.

Comandos avanzados de SNMP

La evolución de SNMP puede verse en los comandos **GetBulk** e **Inform**. **GetBulk** le facilita al agente la búsqueda de información de MIB desde varias instancias de objeto. **Inform** facilita el uso de una jerarquía de NMS para manejar interconexiones complejas, como las que se muestran en la figura 13-17.

El soporte de SNMP a protocolos más allá de IP es un cambio sustancial. Hacer esto extenderá el alcance de SNMP en topologías que no son de IP. Esto es un avance importante para los administradores de redes que están supervisando interconexiones de varios protocolos. No olvide que grandes partes de muchas interconexiones sofisticadas ejecutan

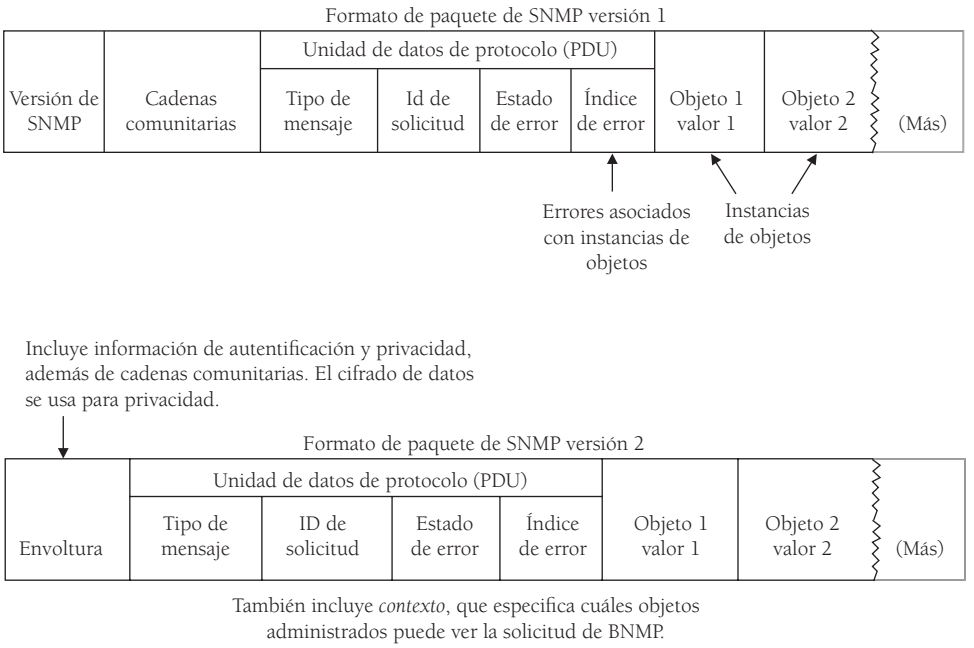


Figura 13-17. La SNMP versión 2 destaca la flexibilidad y la seguridad.

arquitecturas de redes heredadas, como Novell NetWare IPX, AppleTalk y DECnet, y seguirá haciéndolo en el futuro cercano. El soporte extendido al protocolo SNMP llevará esas topologías bajo el control de NMS centralizados.

Comparación entre las versiones 1 y 2 de SNMP

El registro de los estándares puede ser confuso porque se superponen. Por ejemplo justo ahora, casi todas las implementaciones de SNMP son de la versión dos (SNMPv2). Cualquiera que sea la versión, aquí están los componentes del formato de mensaje SNMP:

- **Versión** La versión de SNMP que se está usando.
- **Cadena comunitaria** El equivalente de una contraseña de grupo usada por todos los dispositivos en el mismo dominio administrativo. El mensaje SNMP se ignora sin la cadena comunitaria apropiada.
- **Tipo de Protocol Data Unit (PDU, unidad de datos de protocolo)** Las instrucciones acerca de lo que hay que hacer. La PDU especifica la operación que habrá de realizarse (**GeyBulk**, **Trap**, etcétera) y las instancias de objetos en que se realiza la operación. La PDU está integrada por:
  - **Estado de error** Este campo define un error y un tipo de error.
  - **Índice de error** Este campo asocia el error con una instancia de objeto particular.
  - **Vinculación de variables** No se intimide por el nombre; una vinculación de variable son los datos recolectados en la instancia del objeto (es la carga del paquete SNMP).

SNMPv2 mejora el formato de mensaje con esos cambios:

- ▼ **Envoltura** Esto incluye el destino y los indicadores de la parte de origen para la autentificación y la privacidad del mensaje SNMP, y también identifica el contexto en la forma de los objetos administrados en que la PDU habrá de realizar su operación.
- ■ **PDU mejorada** Las operaciones **GetBulk** e **Inform**.
- ▲ **Protocolos de transporte múltiple** Originalmente, todos los paquetes SNMP se transmitían a través de UDP (User Datagram Protocol, protocolo de datagrama de usuario). SNMPv2 soporta Novell Netware IPX, AppleTalk DDP y OSI CLNS.

Las mejoras en SNMPv2 reflejan la demanda de controles más poderosos y de una mejor seguridad.

Mejor seguridad para los mensajes SNMP

El soporte para SNMP ha sido impedido por las preocupaciones en la seguridad. Un hacker inteligente, armado con un analizador de protocolos no le gustaría nada más que interceptar mensajes SNMP. En vez de sólo tener descargados los archivos de usuario de alguien, irrumpir en un sistema SNMP arrojaría un plano virtual de la topología de la interconexión.

Hoy día, casi todas las redes dependen de una combinación de listas de accesos y cadenas comunitarias SNMP para asegurar sus sistemas de administración. Si de alguna manera un hacker obtiene la cadena comunitaria para un sistema SNMP, podría recorrer los controles de lista de acceso y recuperar datos de todos los dispositivos de la red. Lo que es peor, saber las cadenas comunitarias de lectura y escritura le permitiría a un hacker modificar la configuración del archivo config en los dispositivos de red de la comunidad. Esto sería una brecha de seguridad devastadora, especialmente si se robaran las cadenas comunitarias en las operaciones **set**, porque pondría en sus manos el control de todos los dispositivos configurados para la administración remota.

Los clientes y los fabricantes han pedido una seguridad SNMP más estricta. Tenga en cuenta que un usuario aquí no necesariamente tiene que ser una persona; podría ser solamente un proceso automatizado (como una solicitud **get**) como parte de una encuesta SNMP. En el formato SNMPv2, la envoltura contiene información de autentificación que identifica a los destinos aprobados y las partes de origen en la transacción SNMP. El protocolo de autentificación está diseñado para identificar la confiabilidad de la parte que origina. Más allá de la autentificación, SNMPv2 permite especificar cuáles objetos administrados pueden incluirse en un mensaje. En la figura 13-18 se presenta un esquema de las medidas tomadas para asegurar mensajes SNMPv2.

SNMPv3

SNMPv1 y SNMPv2 son los perros grandes en el bloque de la administración. Sin embargo, no son perfectos. Como se estableció antes, ninguna versión ofrece características de seguridad lo suficientemente fuertes. Para ser más precisos, ninguna versión puede autentificar el origen de un mensaje de administración ni proporcionar cifrado. Sin autentificación, es posible para los extraños usar funciones SNMP. Sin cifrado, es posible monitorear los comandos de administración de su red.

Debido a estas desventajas, muchas implementaciones de SNMPv1 y v2 permiten la capacidad de sólo lectura. Esto reduce su facilidad de uso para que sirva sólo como monitor de red. Al parecer, SNMPv3 corregirá esta deficiencia.

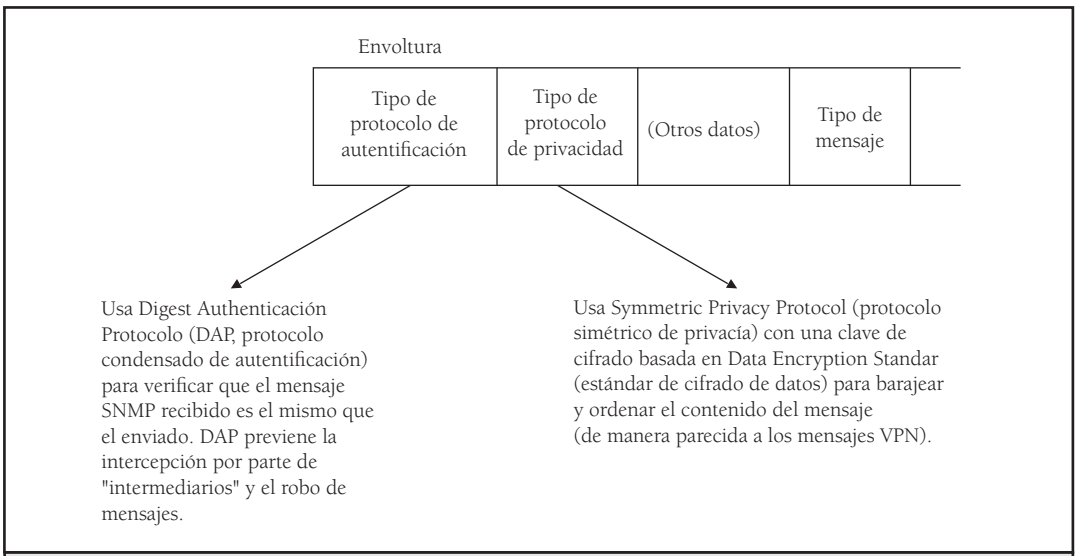


Figura 13-18. Los mensajes SNMPv2 están asegurados por las partes que autentifican y las medidas de control.

La funcionalidad SNMPv3 se ha descrito en los borradores de IETF como "SNMPv2 más administración y seguridad". SNMPv3 agrega tres servicios:

- ▼ **Autentificación** Esto asegura que los comandos SNMP serán emitidos por la persona o la aplicación apropiada.
- ■ **Privacidad** El cifrado permite a los administradores de redes asegurar que sus comandos SNMP no serán espiados.
- ▲ **Control de acceso** Niveles diferentes de acceso para la MIB del agente puede establecerse para diferentes administradores. Los agentes pueden restringir el acceso a sus MIB permitiendo el acceso de sólo lectura o limitando las acciones que pueden tomarse sobre la MIB.

Estos servicios se entregan a través de un concepto llamado *principal*. Se trata de la entidad a cuyo nombre se proporcionan los servicios o tiene lugar el procesamiento. Un principal puede ser un individuo que actúa en cierta función; un grupo de individuos, cada uno actuando en una función determinada; una aplicación o un grupo de aplicaciones; o cualquier combinación de éstos.

Un principal opera desde una estación de administración y utiliza comandos SNMP con los agentes. La identidad del principal y el agente de destino, en conjunto, determinan cuáles características de seguridad habrán de usarse. Debido a que se usa un principal, las directivas de seguridad pueden hacerse a la medida del principal específico, el agente y el intercambio de información, lo que permite flexibilidad al administrador de red.

Cisco integra soporte completo a SNMPv3 a partir de la versión 12.0(3)T. Se implementa para toda las plataformas IOS que tienen imágenes basadas en 12.0(3)T.

SNMP de Cisco e implementaciones RMON

Cisco asegura una capacidad sin paralelo en SNMP y RMON. Casi todos los dispositivos de la empresa cuentan con agentes SNMP, y casi todos los conmutadores incluyen RMON. Como la casa líder de la instancia en el trabajo en Internet, Cisco determina los principales comités en el establecimiento de estándares y se encuentra entre los primeros en lanzar productos que soportan los nuevos estándares.

Cisco y SNMP

Cisco incluye soporte a SNMP en la forma de software de agente en todos los enrutadores y servidores de comunicaciones que fabrica. De acuerdo con la compañía, sus agentes SNMP pueden comunicarse con éxito con OpenView y NetView. Cisco soporta más de 400 objetos MIB. Sus objetos privados MIB presentan soporte para todos los protocolos importantes de LAN, incluidos IP, Novel NetWare IPX, Banyan VINES, AppleTalk y DECnet.

Cisco usa su MIB privado para mejorar el monitoreo de sistemas y la administración de dispositivos de Cisco. Por ejemplo, los enrutadores de Cisco pueden consultarse por la interfaz y el protocolo. Puede consultar el número de paquetes desplazados en una interfaz de red o una consulta para el número de paquetes IPX enviados y recibidos de esa interfaz. Este tipo de información es invaluable para fijar líneas de base para el perfil de tráfico de una red. Las estadísticas de uso promedio de CPU son muestreadas en intervalos de cinco segundos, un minuto y cinco minutos para evaluar si un enrutador se está utilizando de manera apropiada. Las variables físicas también se miden. La temperatura del aire que entra y sale de un dispositivo o las fluctuaciones de voltaje pueden monitorearse para asegurar la operación continua del dispositivo. Las MIB privadas de Cisco incluyen objetos de chasis para reportar el número de módulos instalados, tipos de módulos, números de serie, etcétera. En la figura 13-19 se describen algunas de las características avanzadas SNMP de Cisco.

Para ayudar a asegurar los mensajes SNMP, IOS proporciona la capacidad de prohibirlos de ciertas interfaces que los recorren. SNMP está aun más asegurado por la opción de designar ciertas cadenas comunitarias como de sólo lectura o de escritura-lectura, lo que restringe la capacidad de configurar ciertos dispositivos de manera remota. Además, a un dispositivo puede asignársele más de una cadena comunitaria, lo que permite que enrutadores o conmutadores clave caigan bajo varios regímenes de SNMP (que a veces se utilizan en grandes interconexiones).

Cisco se ha comprometido con hacer sus enrutadores "bilingües" en su soporte simultáneo de SNMPv1 y SNMPv2. La estrategia de coexistencia usa dos técnicas (un agente de proxy que traduce mensajes entre versiones, y el soporte de ambas versiones una sola plataforma NMS).

Cisco y RMON

Cisco integra RMON en todas sus plataformas. Las mayores capacidades están empaquetadas en el Catalyst 6500 de alto rendimiento, pero la capacidad de RMON está integrada también en las tarjetas de la línea de conmutadores LightStream ATM.

Conmutadores RMON para Catalyst El Catalyst actúa simultáneamente como conmutador LAN y una sonda de red, debido a su diseño de varios procesadores. Una CPU hace la conmutación y la otra maneja la colección de datos administrada y reenvía las tareas. El Catalyst puede configurarse para reunir datos de tráfico de una de dos maneras:

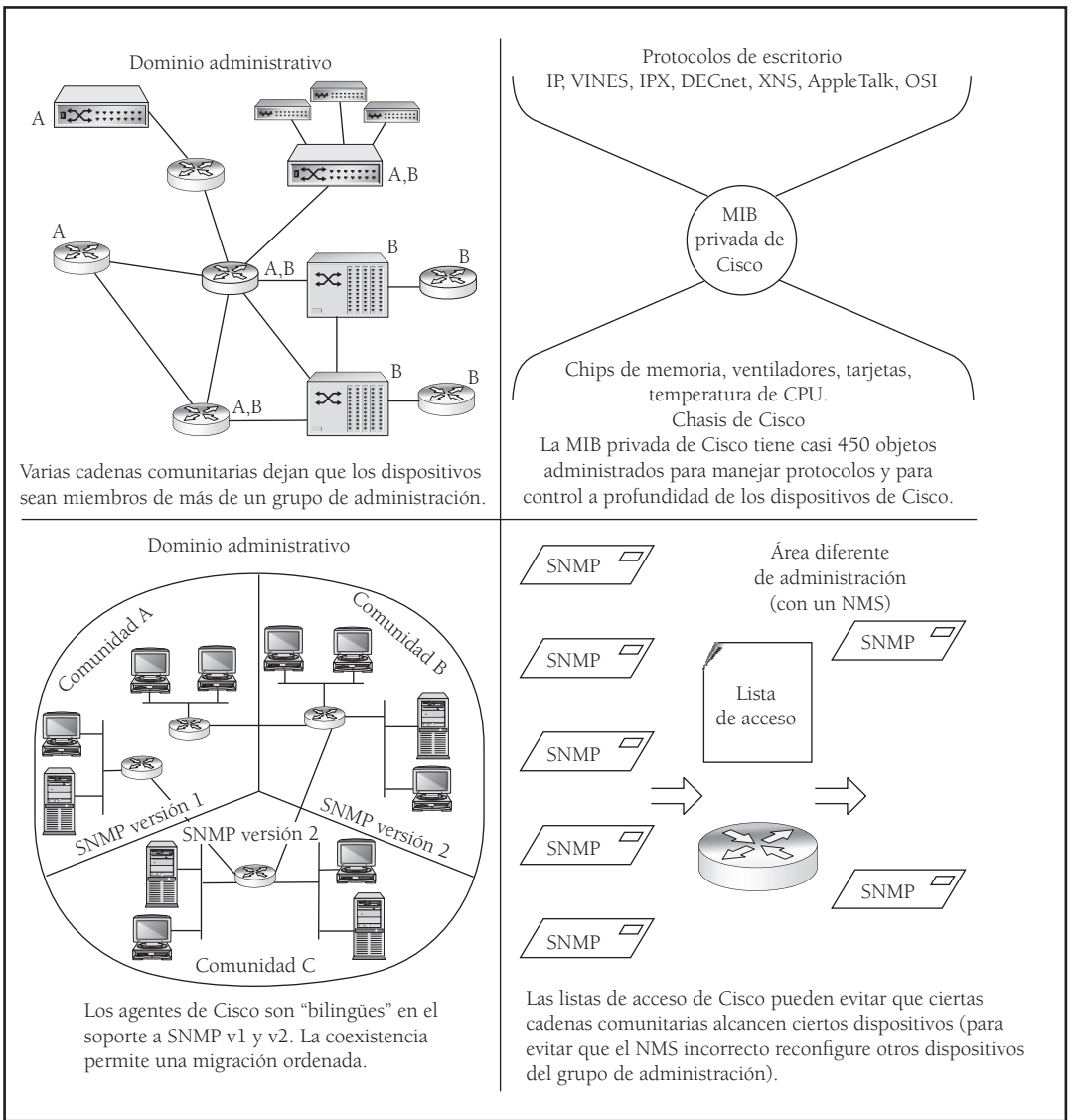


Figura 13-19. La implementación SNMP de Cisco soporta varias funciones avanzadas.

- ▼ **Modo RMON estándar** El agente RMON reúne datos para un máximo de nueve grupos RMON en todos los puertos conmutados que están conectados.
- ▲ **Modo RMON de viaje sin destino** Un modo concentrado que reúne datos más detallados para uno o dos grupos RMON en los ocho puertos, y que se concentra en una sola LAN cuando un evento tiene lugar allí.

En cualquier modo, el RMON permite un curso de acción estructurado para imponer umbrales, generar eventos y enviar alarmas. En la figura 13-20 se describe la estructura.

La configuración RMON concurrente en el modo normal. Su capacidad para ver entre las LAN conectadas es particularmente valiosa para detectar y solucionar problemas, sobre todo en aplicaciones cliente-servidor en que los hosts que comunican están en LAN diferentes.

El transporte sin destino de Catalyst ya es lo suficientemente avanzado. Por lo general, funciona recolectando información histórica detallada en un nivel por puerto y por host. Pero cuando se envía una trampa, el RMON simple, en dos grupos, abarcan una sonda RMON de nueve grupos completamente configurada que empieza automáticamente a recolectar datos para detección y solución de problemas desde la LAN conectada que está causando el problema. En la figura 13-21 se describe cómo un RMON que viaja sin destino cambia para manejar un evento.

Para el momento en que la administrador responde a la alerta, el RMON que viaja sin destino ya se reconfiguró a sí mismo y empezó el monitoreo intenso del segmento de la LAN en que surgió el problema.

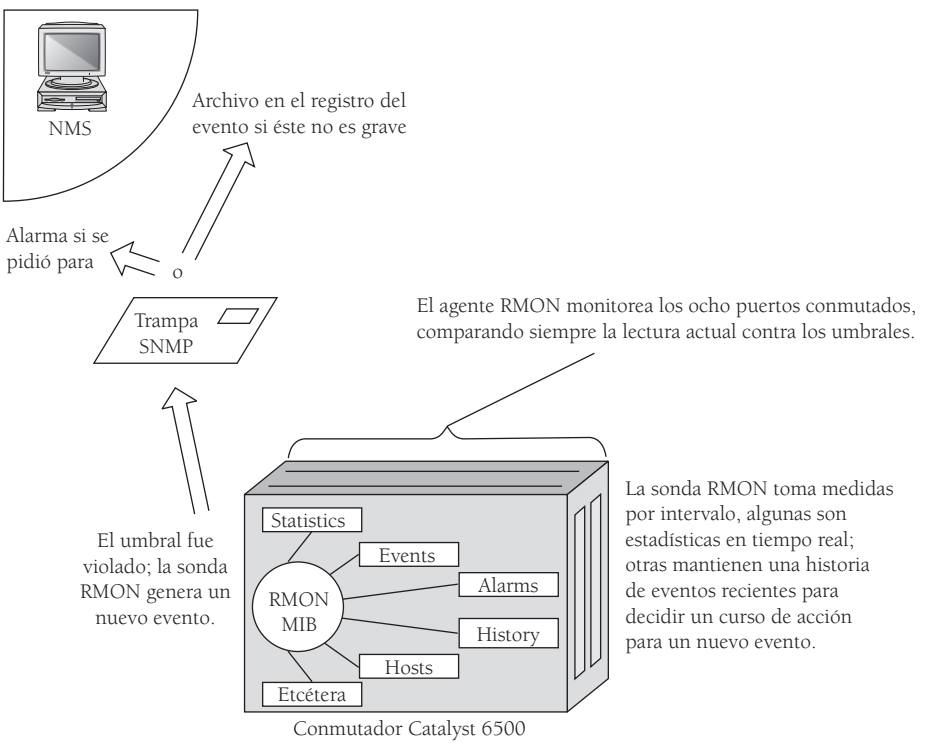


Figura 13-20. Así es como trabajan un RMON conmutado de Catalyst.

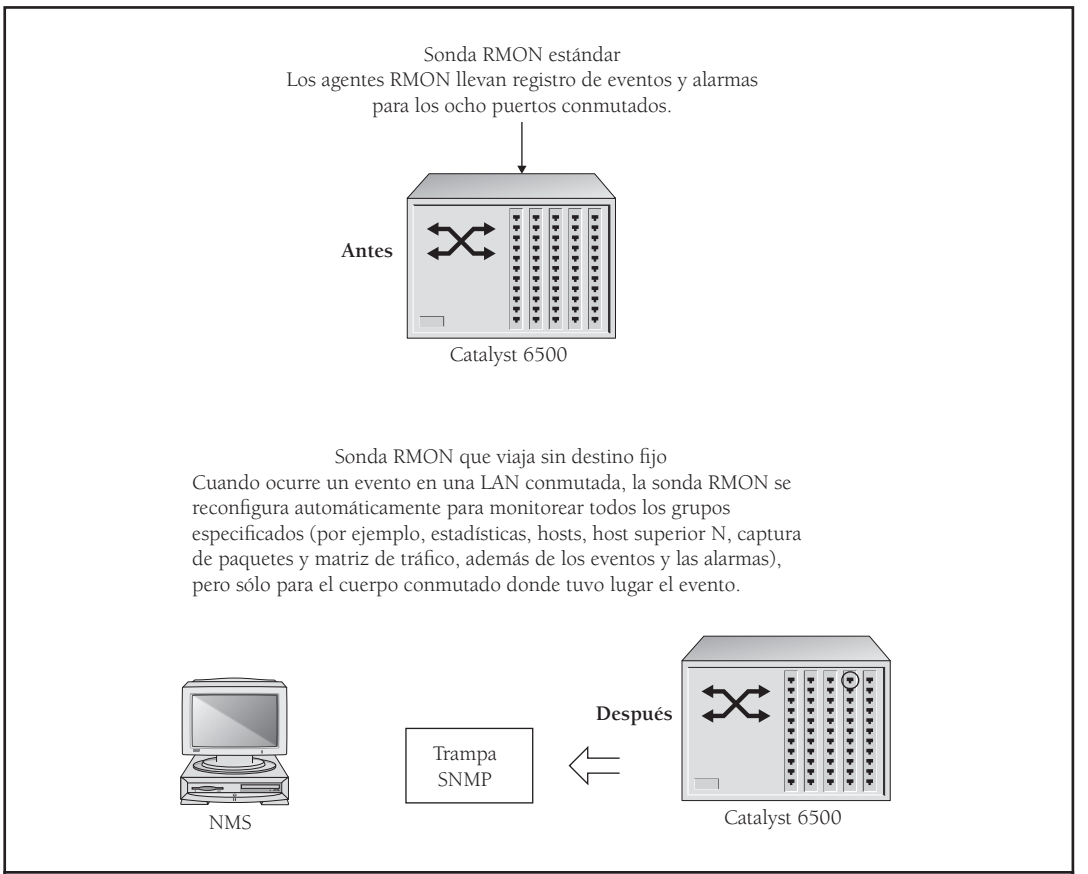


Figura 13-21. El RMON que viaja sin destino impone la instrumentación para concentrarse en el problema emergente.

CISCO NETWORK ASSISTANT (ASISTENTE PARA REDES DE CISCO)

La insignia de la administración de redes Cisco es CiscoWorks. La aplicación (en realidad un conjunto de aplicaciones de administración) es útil y vale la pena. Sin embargo, viene con una etiqueta de precio bastante pesada (cuesta más de 20 000 dólares).

Hechos también y es adecuado para una corporación grande que tiene el presupuesto para pagar una herramientas como ésta (y la necesidad de administrar muchos dispositivos). Las compañías más pequeñas tal vez no tengan el presupuesto ni la necesidad de un conjunto robusto de herramientas como CiscoWorks. Sin embargo, eso no los deja desamparados cuando se trata de aplicaciones de administración de red. Cisco Network Asistan (CNA, asistente para redes de Cisco) es una herramienta que puede ayudarlos.

CNA 4.0 es una aplicación de administración de redes basada en PC para organizaciones pequeñas y medianas con redes de hasta 250 usuarios. La herramienta presenta administración de red y configuración de dispositivo desde una ubicación centralizada.

¿Cuánto cuesta esta aplicación? Eso es lo mejor. Es gratuita.

Características

CNA utiliza una GUI (Graphical User Interface, interfaz gráfica de usuario), de modo que los conmutadores, enrutadores y puntos de acceso de Cisco pueden configurarse y administrarse fácilmente. Entre las características del CNA se incluyen:

- Administración de configuración.
- Información de detección y solución de problemas.
- Inventario.
- Registro de eventos.
- Seguridad de red.
- Sincronización de contraseñas.
- Actualizaciones de IOS.

CNA administra *comunidades* de dispositivos. Las comunidades son grupos de hasta 20 dispositivos de red. Los dispositivos usan el Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco) para identificar dispositivos de red calificados ("calificados" significa que son dispositivos de Cisco). Una vez que un dispositivo se añadió a la comunidad, se vuelve un *dispositivo miembro*.

Debido a que cada dispositivo miembro se administra, monitorea y configura individualmente, debe tener su propia dirección IP.

Las comunidades pueden sonar muy parecido a los conjuntos o grupos. Sin embargo, hay algunas distinciones importantes entre ellas. En primer lugar, los grupos sólo pueden soportar hasta 16 dispositivos, mientras que las comunidades pueden soportar hasta 20. En segundo lugar, sólo los conmutadores pueden agruparse. Las comunidades permiten la inclusión de AP, enrutadores, conmutadores y otros dispositivos de red.

Además, CNA puede comunicarse seguramente con cada dispositivo de una comunidad. En un grupo, las comunicaciones sólo son posibles entre CNA y el dispositivo del comando (el conmutador principal en el grupo).

Las comunidades ofrecen más soporte de recuperación de fallas que los grupos. Si un dispositivo de comandos falla, CNA no podrá administrar cualquier otro dispositivo en el grupo. Sin embargo, usando las comunidades, CNA puede administrar cualquier otro dispositivo de la comunidad en el caso de que otro dispositivo falle.

Instalación

La instalación de CNA es simple y gratuita. Todo lo que necesita es una cuenta en www.cisco.com. No se preocupe (una cuenta en www.cisco.com también es gratuita); todo lo que necesita es llenar algunos formularios en línea y podrá descargar el CNA de inmediato.

Requisitos del sistema

Antes de que descargue CNA, debe asegurarse de que la computadora que habrá de ejecutarlo tiene la velocidad suficiente. En la tabla 13-2 delinea los requerimientos del sistema.

Característica	Requerimientos
Procesador	1 GHz
Memoria	256 MB mínimo, 512 MB recomendado
Espacio en disco duro	70 MB mínimo, 200 MB recomendado
Colores	65 536
Resolución de pantalla	1 024 x 768
Sistemas operativos soportados	Windows XP Service Pack 1 o posterior Windows 2000 Service Pack 3 o posterior

Tabla 13.2 Requerimientos del sistema para el Cisco Network Assistant 4.0.

Sin embargo, esté consciente de que CNA sólo está disponible para Windows XP y 2000 por el momento.

Cómo

Para instalar CNA siga estos pasos:

1. Vaya a www.cisco.com/go/NetworkAssistant.
2. Localice y descargue el instalador de CNA: cna-windows-k9-installer-4-0.exe.
3. Haga doble clic en el instalador en su computadora, y siga las instrucciones en pantalla para completar la instalación.
4. Una vez instalado, haga doble clic en el icono **Cisco Network Assistant** en su escritorio, o localícelo en el menú Inicio.

Vistas

Hay dos maneras en que puede ver su comunidad y sus dispositivos. CNA ofrece las vistas Front Panel y Topology.

Vista Front Panel

La vista Front Panel se usa para administrar la configuración de puerto y los detalles de configuración de uno o más dispositivos. Esta vista de un conmutador Cisco Catalyst 2950 se muestra en la figura 13-22.

Para acceder a la vista Front Panel haga clic en Front Panel de la barra de herramientas, o haga clic en **Monitor | View | Front Panel**.

Esto despliega el panel frontal del dispositivo. Si el dispositivo pertenece a una comunidad, todos los dispositivos que se seleccionaron la última vez que la vista Front Panel fue desplegada aparecen para una comunidad. Y si se trata de un dispositivo de comandos de un grupo, los miembros del grupo que fueron seleccionados la última vez que la vista se seleccionó habrán de desplegarse.

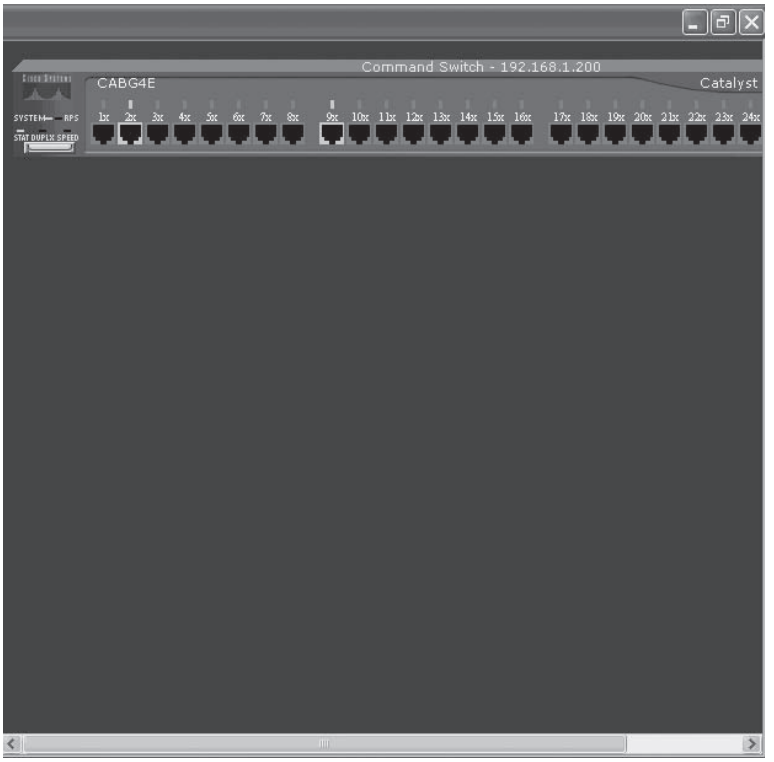


Figura 13-22. La vista Front Panel del Cisco Network Assistant le da una visión general del estado del dispositivo.

La vista Front Panel le permite:

- Reorganizar dispositivos.
- Seleccionar y configurar dispositivos.
- Configurar puertos individuales.
- Configurar varios puertos en varios dispositivos al mismo tiempo.

Vista Topology

Mientras que la vista Front Panel le permitirá examinar un dispositivo o varios dispositivos específicos, la vista Topology muestra la membresía completa de su comunidad o grupo. Esta vista es la predeterminada. Si necesita regresar a la vista una vez que se encuentre en Front Panel, haga clic en Topology View de la barra de herramientas, o haga clic en **Monitor | View | Topology**.

La vista Topology le permite ver los vínculos de VLAN y agregar o eliminar dispositivos de la comunidad.

En la figura 13-23 se muestra la vista Topology de una red pequeña con un conmutador y un AP.

Interacción

CNA le permite configurar y administrar dispositivos de varias maneras. En esta sección se explican las diversas maneras en que puede interactuar con CNA.

Modos Guide y Expert

Las dos maneras fundamentales de interactuar con CNA son a través de los modos Guide y Expert.

El modo Guide está orientado más a los principiantes, porque le lleva a recorrer los pasos de la configuración y administración al mismo tiempo. El modo Expert presenta todas las opciones de configuración a la vez.

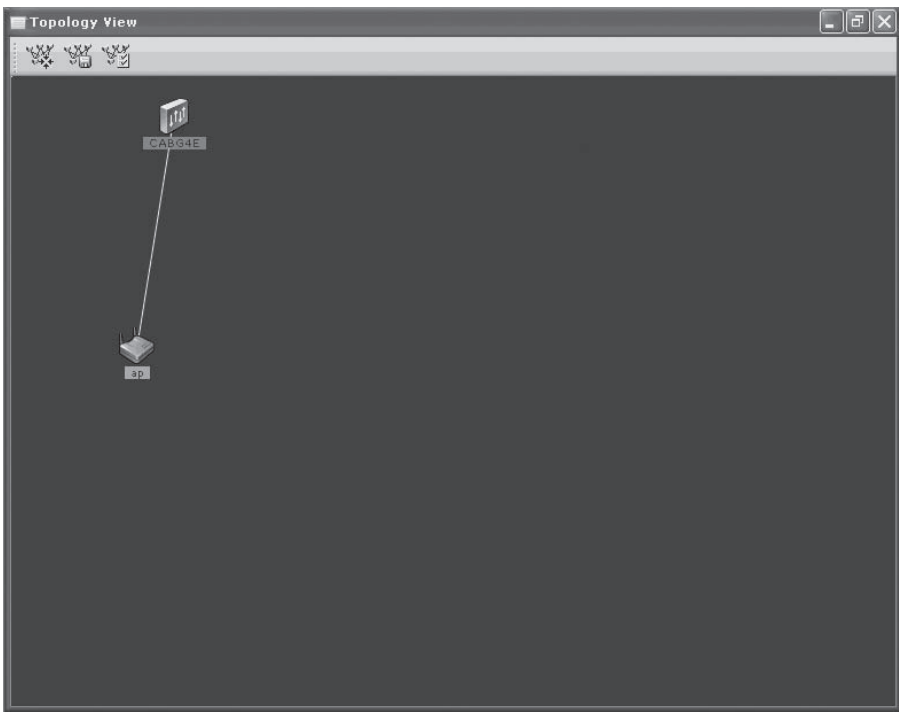


Figura 13-23. Vista Topology del Cisco Network Assistant muestra un diagrama de sus dispositivos administrados de red.

Como opción predeterminada, CNA se encuentra en modo Expert. Al hacer clic en una característica en la barra Feature que muestra un icono de señalización, como se muestra en la figura 13-24, le llevará al modo Guide.

Si selecciona una característica sin este icono, estará en el modo Expert.

Asistentes

CNA también ofrece varios asistentes que le ayudarán con las configuraciones de administración. Los asistentes son como el modo Guide porque tienen el objetivo de simplificar el proceso de configuración. Sin embargo, son diferentes de este modo porque no le tienen toda la información. En cambio, le piden información mínima y llenan los espacios con las configuraciones predeterminadas.

Smartports Advisor (consejero de puertos inteligente)

Smartports Advisor usa configuraciones predefinidas, o *funciones*, para dispositivos. Cuando CNA inicia, revisa si ya se han aplicado Smartports al dispositivo. Si no se han aplicado, CNA le pregunta si quiere que esas funciones se apliquen a sus dispositivos.

Smartports le ayuda a configurar sus dispositivos con seguridad óptima, disponibilidad, calidad de servicio y facilidad de manejo.

Figura 13-24. Los iconos de señalización, en la barra Feature muestran elementos que pueden administrarse en el modo Guide.

Smartports Advisor le muestra los dispositivos a los que está conectado, y luego se muestran los puertos a los que se han aplicado las funciones. También se muestran los puertos a los cuales se podrían aplicar funciones de Smartports.

Comunidades

Una vez que ha instalado e iniciado CNA, puede conectarse a una comunidad existente o un dispositivo. También puede crear una nueva comunidad.

Conexión

Cuando inicia CNA, usa la ventana Connect, como se muestra en la figura 13-25, para conectarse a un dispositivo específico o una comunidad existente.

Para conectarse a una comunidad existente haga clic en la opción **Connect to a new community**.

Para conectarse a una comunidad específica, haga clic en la opción **Connec to**, y luego seleccione la comunidad de la lista desplegable.

Para conectarse a un grupo específico, seleccione la dirección IP del dispositivo del comando del menú desplegable.

Al hacer clic en el botón **Options**, se le permite:

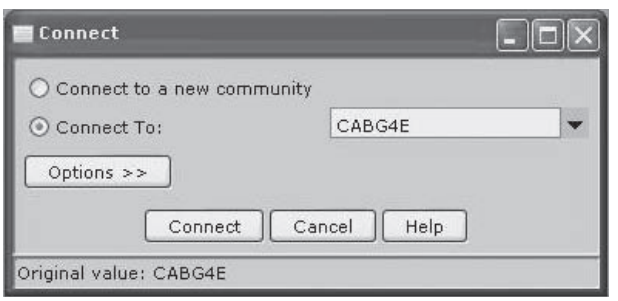


Figura 13-25. La ventana Connect le permite seleccionar la comunidad con la que habrá de conectarse.

- ▼ Comunicarse con un dispositivo independiente o un dispositivo de comandos del grupo empleando HTTPS en lugar de HTTP y seguro.
- ■ Utilizan un puerto HTTP diferente a 80.
- ▲ Conectarse con acceso de sólo lectura.

Una vez que ha seleccionado la comunidad a la que quiere acceder, se le pedirá un nombre de usuario y contraseña.

Si se está conectando a un grupo, CNA le pregunta si le gustaría convertir el grupo en una comunidad. Simplemente ingrese la dirección de IP del dispositivo de comandos del grupo, y CNA lo convertirá. No se preocupe si quiere retener las propiedades del grupo. CNA no eliminará esa información, y aún podrá usarla como parte de un grupo.

Planeación

Aunque CNA es más bien amigable con el usuario, no deja de tener sus limitaciones y reglas para el desarrollo de sus propias comunidades.

Como ya se indicó antes, una comunidad no puede exceder de 20 dispositivos. Una vez dicho eso, hay un número máximo de cada dispositivo específico que puede incluirse. En la tabla 13-3 se detalla el número máximo de dispositivos específicos permitidos dentro de cada comunidad.

Cuando exceda el número de dispositivos máximos permitidos, se abrirá una ventana y le indicará cuántos dispositivos de cada tipo tiene. No podrá administrar la comunidad hasta que obtenga el número apropiado de dispositivos.

Pero, ¿qué pasa si tiene muchos dispositivos? La respuesta es sencilla: sólo cree una nueva comunidad. No hay límite en el número de comunidades que puede administrar con CNA.

Descubrimiento

Cuando inicia CNA, ingrese la dirección IP de uno de sus dispositivos (como se muestra en la figura 13-26) y, usando CDP, CNA descubrirá todos los dispositivos de Cisco en su red. CNA también puede descubrir dispositivos entre varias redes y VLAN, suponiendo que tengan direcciones IP válidas.

Dispositivo	Máximo permitido
Conmutadores Catalyst no modulares	16
Conmutadores Catalyst modulares	4
Enrutadores de acceso	2
Firewalls PIX	2
Puntos de acceso	Ilimitado

Tabla 13-3. Número máximo de dispositivos permitidos en una comunidad.

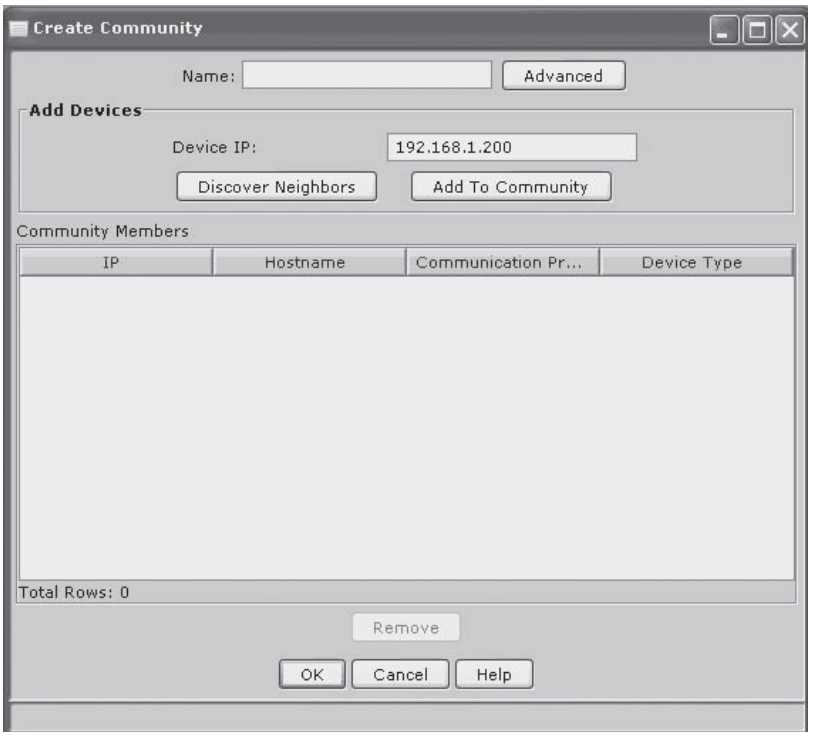


Figura 13-26. Ingresé la dirección IP de uno de sus dispositivos para empezar el proceso de descubrimiento.

Una vez que CNA ha descubierto todo los dispositivos en su red, puede ordenarlos para colocarlos en la comunidad o en las comunidades que desee.

NOTA No necesitará nombres de host para los dispositivos cuando use CNA. Sin embargo, IOS asigna automáticamente a los conmutadores el nombre de host "Switch". Tal vez quiera cambiar el nombre de sus conmutadores antes de ejecutar CNA, simplemente para saber con mayor facilidad cuál conmutador es cuál.

Se le preguntan las contraseñas sólo cuando una contraseña ya ingresada no funcione en un dispositivo determinado. Por ejemplo, si tiene 20 dispositivos y todos ellos tienen la misma contraseña, sólo tendrá que ingresar la contraseña una vez. Sin embargo, si todos tienen diferentes contraseñas, tendrá que ingresar 20 contraseñas distintas.

Creación

Las secciones antes mencionadas fueron útiles cuando se conectaba a una comunidad existente, pero es probable que necesite crear su propia comunidad antes de empezar.

Las comunidades pueden crearse de una de tres maneras:

- ▼ Descubriendo y agregando dispositivos.
- ■ Creándolos manualmente.
- ▲ Convirtiendo un grupo.

Descubrimiento y adición de dispositivos Para tener una lista de dispositivos candidatos y luego agregarlos a su comunidad:

1. Inicie CNA.
2. Seleccione **Connect to a new community** en la ventana Connect.
3. Haga clic en **Connect**.
4. En la ventana Create Community, ingrese un nombre para su comunidad.
5. Si quiere seleccionar un puerto HTTP diferente del 80, haga clic en el botón **Advanced**, y luego haga clic en **OK**.
6. Ingresé la dirección IP para el dispositivo en su red.
7. Haga clic en **Discover Neighbors**.
8. En la lista Devices Found, seleccione los dispositivos que desea eliminar.
9. Haga clic en **Remove**.
10. Para agregar los dispositivos restantes a su nueva comunidad, haga clic en **Add All Yo Community**.

Adición manual de miembros Hay dos maneras en que puede agregar manualmente dispositivos miembros a una comunidad:

- ▼ En la ventana Create Community, ingrese la dirección IP del dispositivo, y luego haga clic en **Add to Community**.
- ▲ La segunda manera utiliza la vista Topology. Haga clic con el botón derecho en el icono de un dispositivo candidato, y seleccione **Add to Community** del menú contextual resultante.

NOTA Los miembros de una comunidad están etiquetados en verde, mientras que los dispositivos candidatos están en cian.

Conversión de un grupo Si quiere convertir un grupo en una comunidad desde la aplicación, haga clic en **Configure | Cluster | Cluster Conversion Wizard**.

Uso de CNA

Una vez que esté conectado a su comunidad, todo lo que necesita hacer para usar CNA es navegar por la GUI. En esta sección, se examina la configuración y administración de un conmutador Catalyst 2950.

Hay muchas maneras de manejar las diferentes configuraciones y ventanas descritas en esta sección. Fijaremos nuestra atención en el panel de la izquierda (también llamado la barra Feature) en CNA. Ésta contiene las diferentes configuraciones que podemos administrar, pero muchas también pueden establecerse al hacer clic en un icono en la parte superior de la pantalla o desde un menú contextual en algún lugar dentro de la aplicación. Para tener consistencia, hablaremos sobre los atributos tal como se acceden desde la barra Feature.

Configuración

La parte Configure de la herramienta CNA le permite administrar características como:

Ports Esta ventana le permite administrar las configuraciones de puerto y los EtherChannels. En la figura 13-27 se muestra la ficha Configuration Settings de Port Settings. Para hacer un cambio basta con hacer clic con el botón derecho en un atributo y seleccionar la nueva configuración del menú desplegable.

La ficha Runtime Status muestra el estado actual del dispositivo.

La selección de EtherChannels le permite administrar las configuraciones de EtherChannels para este dispositivo.

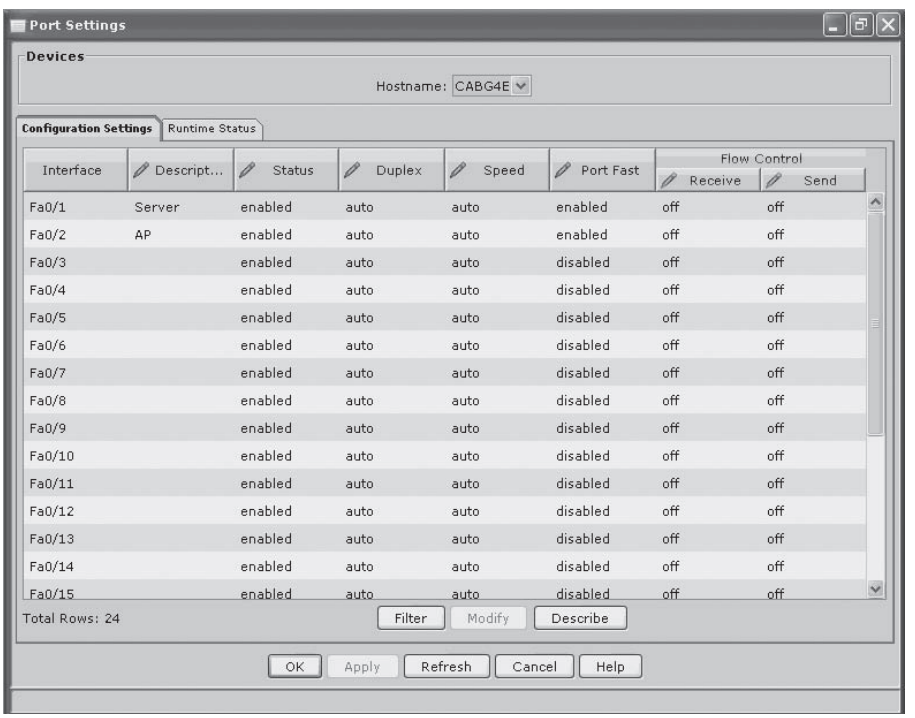


Figura 13-27. Port Settings es donde puede administrar atributos de los puertos de su dispositivo.

Seguridad La seguridad del puerto se maneja con la configuración de Port Security. Esta ventana tiene dos fichas:

- ▼ **Security Configuration** Se usa para revisar la configuración de seguridad del puerto y configurar un puerto seguro. Los puertos seguros son aquellos donde una acción especificada por el usuario inicia cada vez que ocurre una violación de la seguridad en una dirección.
- ▲ **Secure Address** Se usa para agregar, eliminar o administrar direcciones seguras. Se trata de direcciones MAC que se reenvían únicamente a un puerto por VLAN.

Para administrar esta configuración, seleccione un dispositivo de la lista Hostname cuya configuración de seguridad quiera administrar.

Puede filtrar los resultados de la lista al hacer clic en Filter y usar la ventana Filter Editor.

Calidad del servicio La configuración de Quality of Service (QoS, calidad del servicio) se administra con este atributo. Los paquetes entrantes contienen un valor de Class of Service (CoS, clase de servicio) entre 0 y 7, o un valor de Differentiated Services Code Point (DSCP, servicios diferenciados de punto de código) entre 0 y 63.

Usted decide cuál marcador quiere confiar y que valor predeterminado de CoS asigna a un paquete si no contiene un marcador. Esto se hace al seleccionar Trust Settings bajó la configuración Quality of Service. La venta resultante también se muestra en la figura 13-28.

Conmutación Este atributo le permite configurar varias características de su conmutador. Las características que se muestran aquí son singulares a las capacidades de configuración del Cluster Management Suite (CMS, suite de administración de grupos), que se cubrió en el capítulo 5. CNA simplemente proporciona otra manera de configurar esta configuración. También proporciona un entorno en que puede aplicar parámetros de configuración consistentes en todos los dispositivos de una comunidad, o en los dispositivos seleccionados.

Para conocer más información acerca de la configuración de un conmutador, regrese al capítulo 5.

Propiedades del dispositivo La configuración Device Properties le permite administrar elementos básicos del dispositivo como la dirección IP, la información de gateway y los nombres y contraseñas de usuario.

Monitor

La sección Monitor de la barra Feature le permite revisar varios fragmentos de información y estadísticas acerca de su dispositivo. Hay dos partes del atributo monitor: Reports y Views.

Informes La configuración Reports le permite revisar estadísticas de su dispositivo, entre la información se incluye:

- ▼ **Inventory** Le proporciona una lista de dispositivos en su comunidad, junto con el tipo de dispositivo, el número de serie, la dirección MAC, la dirección IP y la versión del IOS.

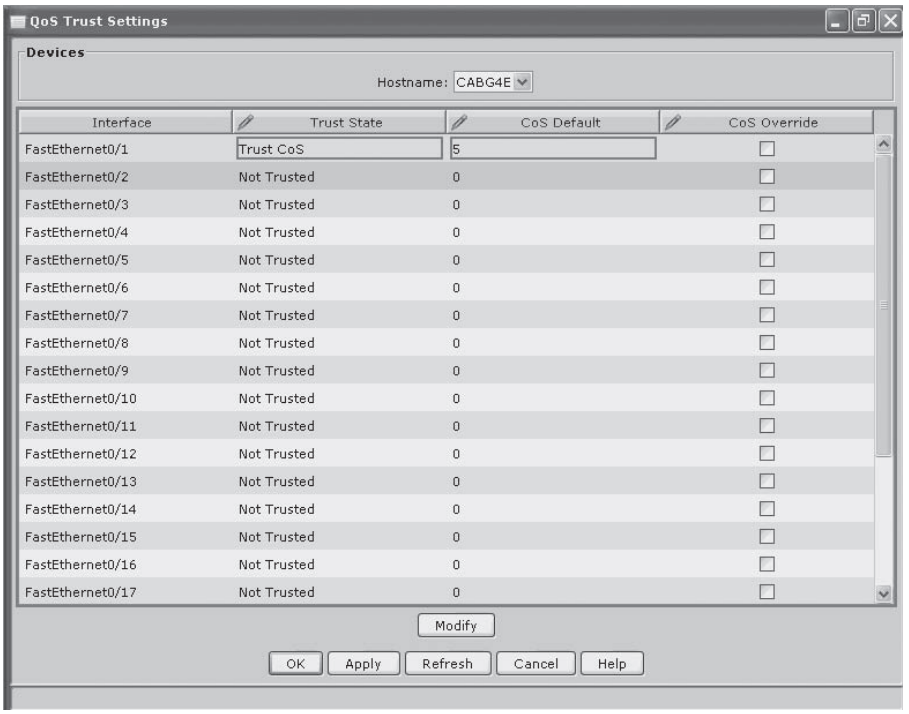


Figura 13-28. La administración de calidad de servicio en el Cisco Network Assistant le ayuda a controlar el flujo del tráfico en la red.

- **Estadísticas de puerto** Le proporciona información acerca las velocidades de transmisión y recepción del puerto.
- **Gráfica de ancho de banda** Proporciona gráficas de línea y de barras que describen el uso del ancho de banda, como la que se muestra en la figura 13-29.
- **Gráficas de vínculo** Proporciona gráficas de línea y de barras que describen las estadísticas de vínculos.
- **ARP** Proporciona una tabla que vincula el dispositivo y su dirección MAC con su dirección IP. La tabla también muestra la edad de la entrada en la tabla, su método de encapsulamiento y la interfaz del dispositivo.

Views Le permite revisar los eventos y los mensajes del sistema. Por ejemplo, la configuración Event Notification le alerta de eventos que CNA considera importantes. Entre estos eventos se incluyen:

- Un dispositivo con una temperatura elevada.
- Un dispositivo con un ventilador roto.
- Un puerto con un dúplex que no coincide.
- Un dispositivo desconocido en la red.

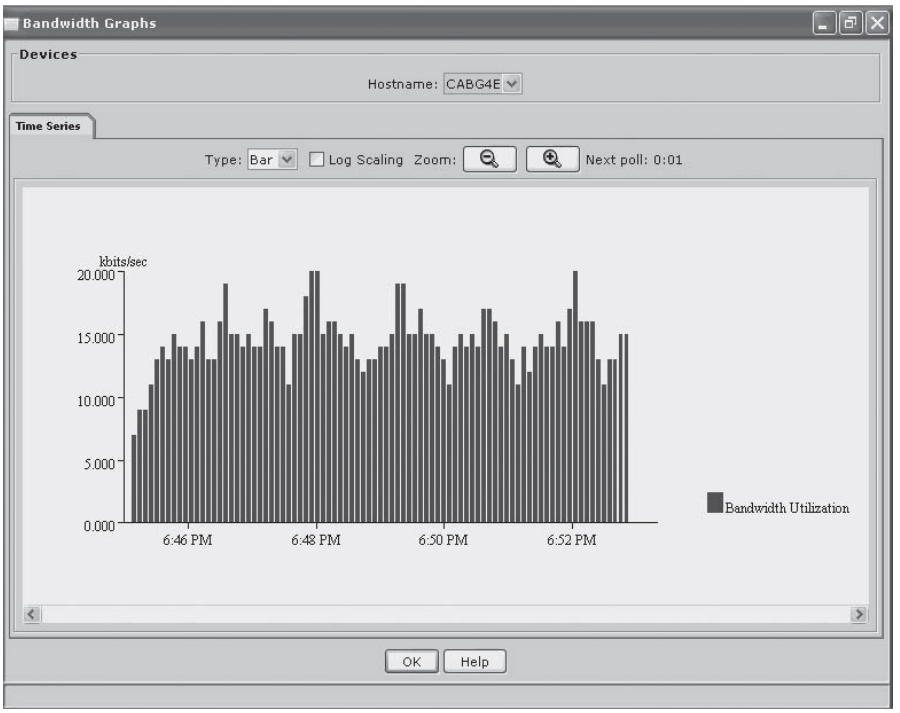


Figura 13-29. Las gráficas de ancho de banda muestran gráficas de línea y de barras que le muestran el uso del ancho de banda.

Los mensajes del sistema pueden configurarse para que le envíen un correo electrónico cuando un mensaje se genera.

Detección y solución de problemas

Si está teniendo problemas con un dispositivo, el atributo Troubleshoot ofrece una característica Ping and Trace.

Puede rastrear una ruta de capa 2 o 3. Una ruta de capa dos determina la ruta de la red de origen o destino de un dispositivo de capa 2. Un rastreo de capa 3 determina la ruta que viaja un paquete en una red de capa 3, pero no incluye la información acerca de los dispositivos de capa 2.

La ventana Ping and Trace se muestra en la figura 13-30.

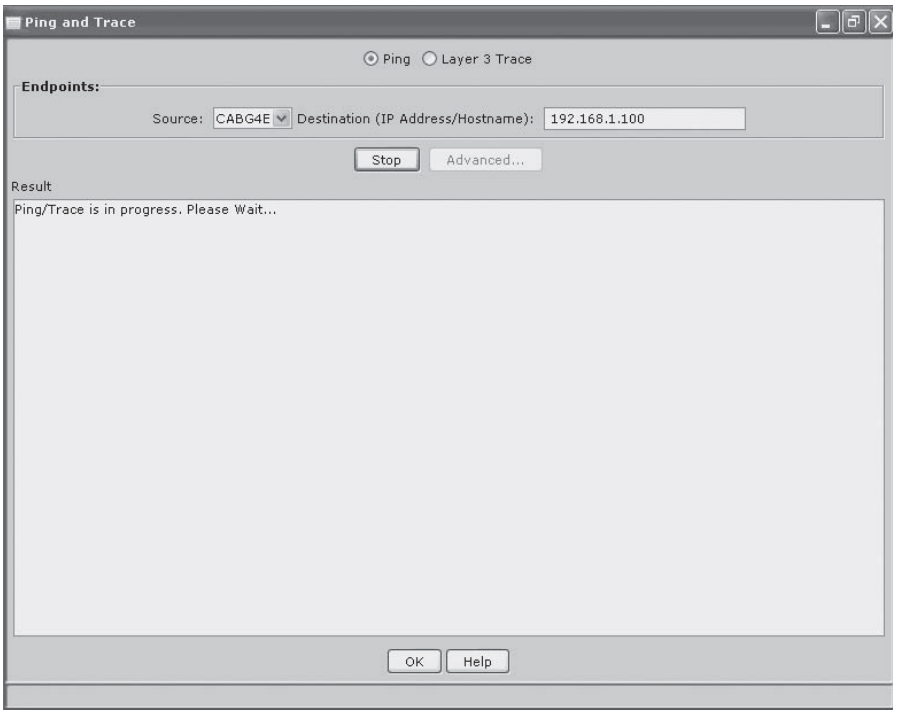


Figura 13-30. Cisco Network Assistant proporciona servicios de Ping and Trace para ayudarle con la detección y solución de problemas.

Mantenimiento

El atributo final es Maintenance, donde se puede administrar la funcionalidad de CNA.

Una de sus mejores características es la capacidad de actualizar el software para los dispositivos de su comunidad. Haga clic en **Software Upgrade**, y se abrirá la ventana mostrada en la figura 13-31.

Esto le permite seleccionar dispositivos específicos en su comunidad que desea que CNA actualice. Cuando selecciona **Upgrade settings**, especifica en qué parte de su computadora o en la red se localiza el archivo actualizado. Los archivos de actualización de sus dispositivos pueden encontrarse en www.cisco.com.

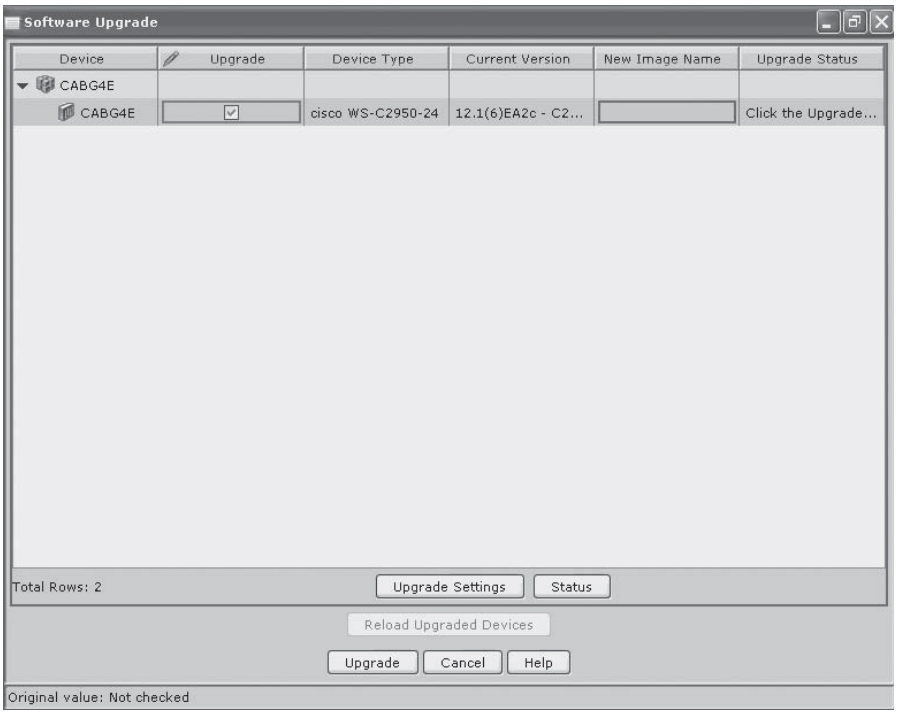


Figura 13-31. El firmware de su dispositivo se actualiza fácilmente utilizando Cisco Network Assistant.

Configuration Archive almacena configuraciones de comunidad y dispositivos antiguas, y System Reload guarda la configuración de dispositivo actual y reinicia el dispositivo.

La administración de red es una tarea increíblemente importante para mantenerlo con vida. El trabajo en una red no se detiene una vez que se ha construido y configurado. Las redes son entornos dinámicos, y es necesario monitorear constantemente el rendimiento de su red y configurar sus requisitos. Felizmente, Cisco ofrece varias aplicaciones para mantenerle adelante del comportamiento de su red.

CAPÍTULO 14

Procesos de diseño de redes

Hasta ahora hemos cubierto los componentes que conforman una interconexión. En este capítulo, pondremos este conocimiento a trabajar al examinar el proceso de diseño de redes y configurar redes para que se adecuen a varios escenarios de diseño.

Como ya ha visto, no son pocas las tecnologías y los productos entre los que se puede elegir (incluso sólo en línea de productos de Cisco). También ha visto cómo no es fácil el trabajo en redes: cada diseño conlleva un equilibrio de un tipo o de otro. Estos equilibrios pueden venir en la forma de ancho de banda reducida para llevar tráfico de carga útil, complejidad aumentada, gastos adicionales u otras desventajas. Cuando se diseña una red, necesita saber no sólo cuáles son las opciones, sino también como jugar con ellas para obtener el mejor equilibrio posible.

Cada año aparecen tantos nuevos productos y avances en tecnología que tan sólo escribir las siglas correctamente es difícil. En este capítulo ordenaremos las cosas un poco al aplicar la línea de productos de Cisco a problemas reales. La revisión de los problemas de configuración de las interconexiones nos ayudará a poner las cosas en perspectiva y concentrarnos en estos intercambios para buscar el equilibrio que resulta crítico.

FUNDAMENTOS DEL DISEÑO DE INTERCONEXIONES

Interconexión tiene una naturaleza geográfica, de modo que casi todas las prácticas de diseño se relacionan con la aplicación de la topología a las necesidades. (Del capítulo 5, recordará que una topología es un mapa del diseño físico de la interconexión.) El diseño de una interconexión determina en gran medida cómo será su rendimiento y qué tan bien podrá escalarse. En las redes, escala, o escalabilidad, significa cuánto puede crecer una interconexión sin tener que cambiar la forma básica de su topología (es decir, sin tener que remplazar o reconfigurar excesivamente una infraestructura existente).

Revisión de los fundamentos de las interconexiones

Ahora viene al caso un recorrido rápido de lo que hemos aprendido hasta ahora. Resulta especialmente importante hacerlo aquí, porque en este capítulo revisaremos una variedad de factores de diseño y opciones. Por tanto, necesitamos tener claros los diversos componentes que integran una interconexión.

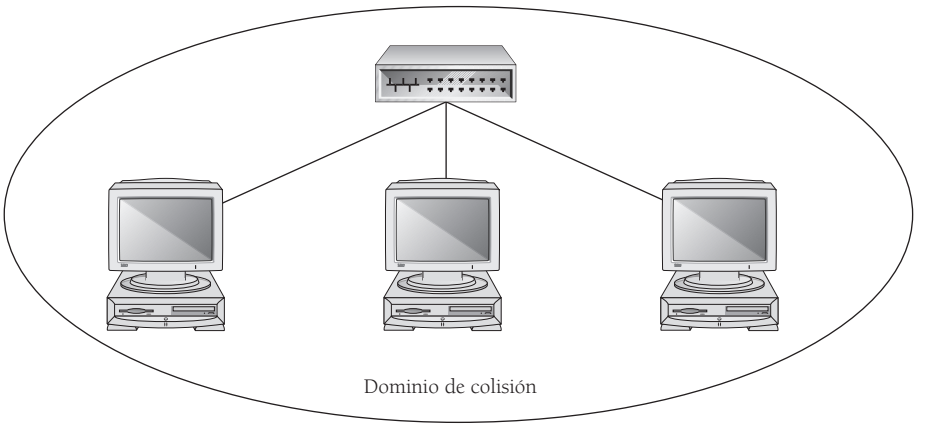
Segmentos LAN

Los conmutadores conforman los segmentos LAN, el bloque de construcción básico de toda interconexión. Cada puerto conmutado es un segmento que recorre un proceso llamado *microsegmentación*. Un segmento LAN podría ser una LAN departamental o una espina dorsal LAN de alta velocidad que sirve a docenas de otros segmentos LAN dentro de una empresa.

NOTA A manera de revisión, un segmento LAN es un medio físico compartido entre un grupo de dispositivos. La mayor parte de los segmentos LAN están formados por concentradores o conmutadores. Estrictamente hablando, un segmento LAN es una LAN. Sin embargo, por lo general, el terminó LAN se utiliza para referirse a una red local que consta de muchos segmentos LAN.

Dominios de colisión y transmisión

Un dominio de colisión es un medio de red compartido que permite que los paquetes Ethernet colisionen; un dominio de transmisión es el área dentro de la cual los mensajes pueden enviarse a todas las estaciones utilizando una denominada dirección de transmisión. Los dominios de colisión deben ser pequeños porque las colisiones limitan el uso del ancho de banda. Cuantos más hosts estén conectados a un segmento LAN, más lento es el desplazamiento del tráfico.



Casi todos los dominios de colisión están formados por concentradores que conectan dispositivos hosts a las interconexiones. Los concentradores son el equivalente funcional de los segmentos de cable Ethernet utilizados en los primeros días de las redes de área local. La colisión de segmentos de conmutadores domina en cada puerto conmutado.

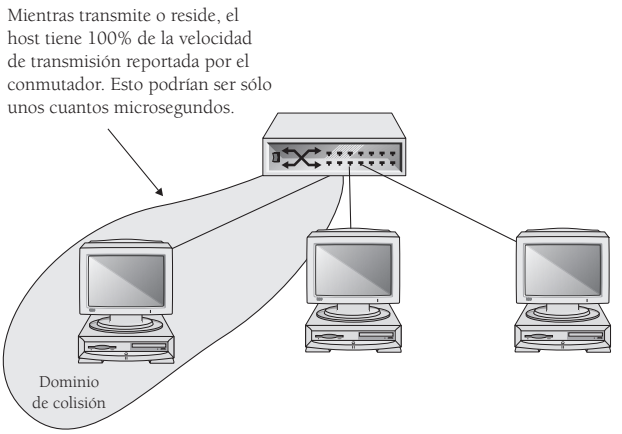
Algunas transmisiones son útiles, pero demasiadas pueden hacer muy lenta una red con una gran cantidad de exceso de tráfico inútil (un fenómeno que no es bienvenido y al que se le domina *tormenta de transmisiones*). Los dominios de transmisión son, como opción predeterminada lo mismo que un dominio de colisión de red para los medios compartidos (en otras palabras, concentradores), pero el alcance de la dirección de transmisión puede hacerse mucho más pequeña que un dominio de colisión utilizando conmutadores. Por lo general, los enrutadores limitarán las transmisiones, pero un dominio de transmisión puede extenderse a configurar un enrutador para dejar que pasen los mensajes transmitidos.

Comparación entre ancho de banda compartido y conmutado

Los conmutadores también conectan hosts a las redes, pero de una manera fundamentalmente diferente. Un conmutador "segmenta el tiempo" de acceso a la red de sus hosts, conectados de manera tal que cada puerto de conmutador forma un canal con un dominio de colisión de uno. A esto se le llama *ancho de banda conmutado*, en oposición al *ancho de banda compartido* de los concentradores. Se estima que las redes conmutadas son diez veces más rápidas que las redes compartidas en el mismo medio.

Más aún, las redes conmutadas soportan LAN virtuales (VLAN), lo que permite a los administradores agrupar usuarios de manera racional en lugar de verse forzados a agruparlos de acuerdo con los dispositivos de host a los que están conectados.

Además de formarlos por hosts de conexión, los conmutadores más grandes conectan segmentos LAN para formar interconexiones. Para evitar confusión, los dos tipos de conmutadores se denominan a veces conmutadores de acceso y conmutadores (o espina dorsal) LAN.

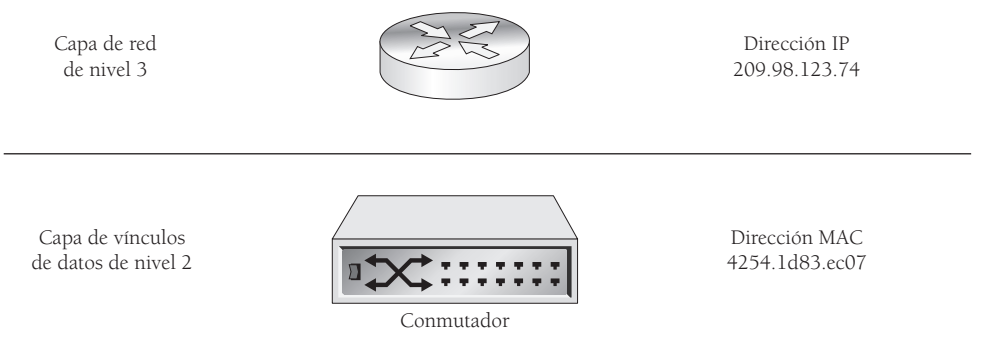


Los enrutadores controlan las interconexiones

El tercer dispositivo básico en la interconexión es el enrutador. Los enrutadores conectan los segmentos LAN en lugar de conectar hosts, como lo hacen los concentradores y los conmutadores de acceso. Los enrutadores se usan para aislar el tráfico intramuros y para proporcionar seguridad interna. Además, pueden extender la transmisión y los dominios de transmisión múltiple a segmentos LAN especificados para ayudar a unir esas redes en una unidad funcional.

Los enrutadores se despliegan tanto dentro de las interconexiones como en la orilla de los sistemas autónomos. Dentro de los enrutadores en ocasiones se encuentran los denominados enrutadores internos o enrutadores de acceso. Los enrutadores que se concentran en la comunicación con el exterior se denominan enrutadores de orilla, o gateway. Por ejemplo, un Internet Service Provide (ISP, proveedor de servicio de Internet) usará enrutadores gateway para conectarse a Internet. En contraste, una empresa grande colocará por lo menos un enrutador interno en cada uno de sus sitios importantes para ayudar a manejar el tráfico interno.

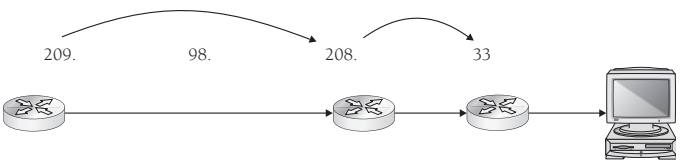
Los enrutadores son más inteligentes que los concentradores y los conmutadores porque pueden interpretar la dirección de red. Leen la dirección de red para filtrar el tráfico, controlar el acceso a las redes o servicios y elegir la mejor ruta para alcanzar un destino. Los enrutadores dan vida a las interconexiones. No es coincidencia que los tres dispositivos más básicos de la interconexión operen en diferentes niveles del modelo de referencia OSI de siete capas, como se ilustra aquí:



Los enrutadores operan en la capa de la red (capa 3). Hoy en día, casi todas las interconexiones usan direcciones de red IP (todos los enrutadores de Internet lo hacen). Pero muchos enrutadores internos aún deben acusar protocolos de escritorio heredados como IPX, AppleTak o DECnet. Por esto, Cisco y sus competidores han invertido mucho en productos de ingeniería de varios protocolos para permitir que las LAN heredadas interoperen con IP. Los conjuntos de características IOS de Cisco existen principalmente para dar a los diseñadores de red opciones en la compra de software de sistema que cubran sus necesidades de protocolo de red.

Los enrutadores usan direcciones de red de capa 3

Sea IP o un protocolo heredado de capa 3, las direcciones de red son inherentemente jerárquicas. Una manera de ver esto es que, a medida que un enrutador se abre camino a través de una dirección IP, se centra en el segmento LAN al que está conectado el host de destino. A través de una gran cantidad de rutas, los movimientos hacia la dirección se manifiestan en saltos entre enrutadores. Una ruta de un salto sólo requiere encontrar el segmento LAN en que reside el destino.



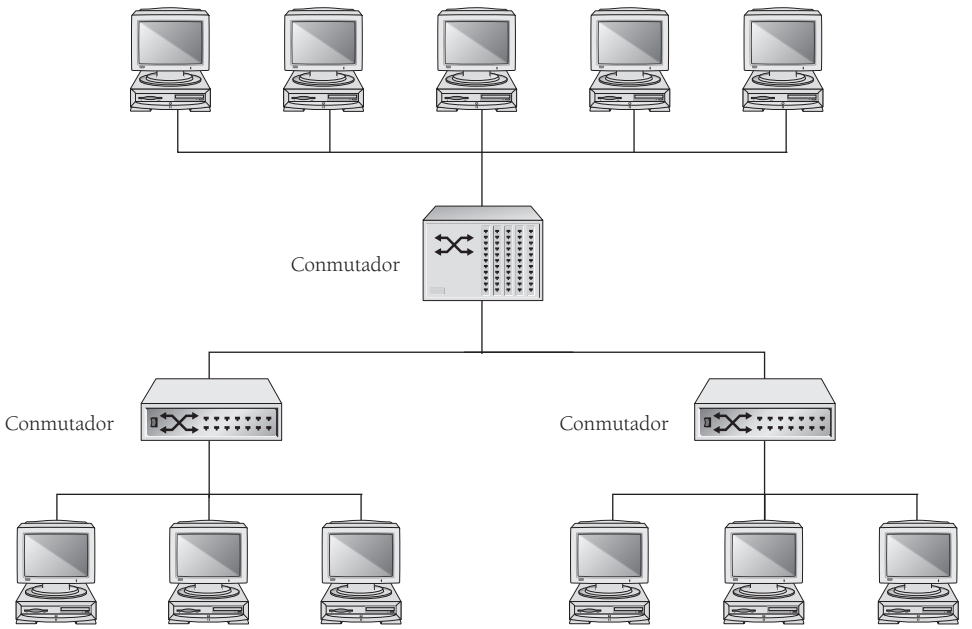
Las rutas a menudo se resumen antes de ser compartidas con otros enrutadores. Esto mejora el desempeño al reducir en gran medida el número de entradas de dirección transportadas dentro de una tabla de ruta de un enrutador. El resumen de ruta, llamada *agregación de ruta*, trabaja al depender de que un enrutador de gataway conozca la dirección completa del segmento LAN de destino y al permitir que enrutadores interinos transporten entradas más pequeñas, resumidas en sus respectivas tablas de enrutamiento, con lo que mejora el desempeño. La traducción de direcciones también se usa con frecuencia, donde las direcciones internas se alteran o agrupan en una dirección global en paquetes enviados fuera de una interconexión. Mecanismos como Port Address Translation (PAT, traducción de dirección de puerto) y Network Address Translation (NAT, traducción de dirección de red) se usan en enrutadores de orilla o firewalls para hacer esas traducciones en el campo de dirección del paquete en ambos sentidos.

Los conmutadores usan direcciones MAC de capa 2

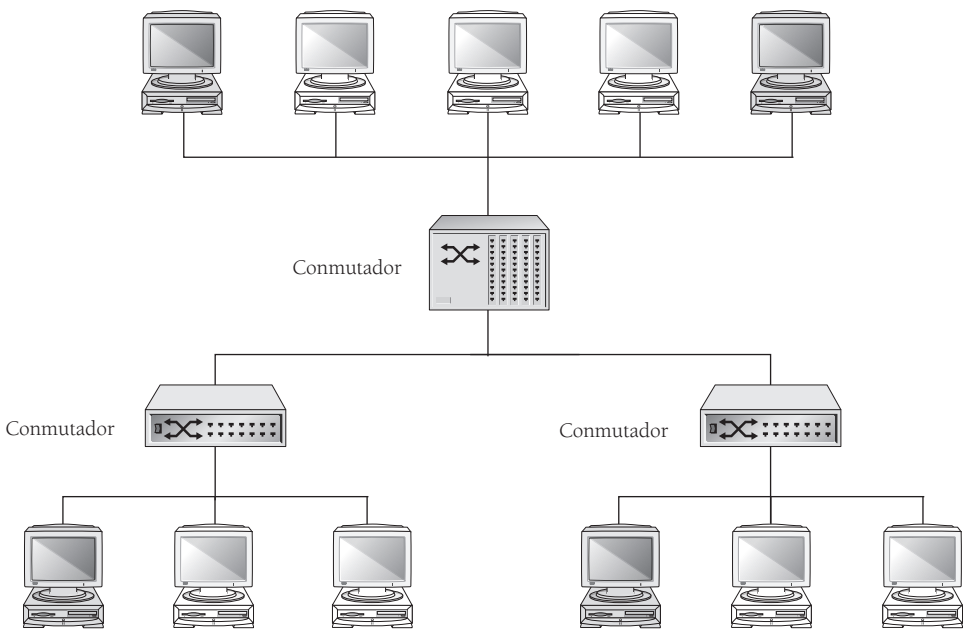
Los conmutadores operan en la capa de vínculo de datos (capa 2), y tratan con direcciones MAC en lugar de direcciones de red. Una dirección MAC es un número largo que identifica de manera única a los dispositivos de hardware físicos. Las MAC combinan el código de un fabricante con un número de serie. Aun los enrutadores gozan direcciones MAC para el último paso de un mensaje (resolviendo una dirección IP en la dirección MAC física para localizar el host de destino dentro del segmento LAN).

Las direcciones MAC son topológicamente planas. El perfil lógico de una dirección MAC aparece como si todos los hosts estuvieran conectados al mismo cable; no ofrece pistas sobre dónde están localizados los hosts porque es básicamente un número de serie. Las re-

des conmutadas, por tanto, deben operar mediante la fuerza bruta, enviando flujos de transmisiones de direcciones MAC a todos los puertos cuando no se conoce un destino MAC.



Zona de flujo de transmisión

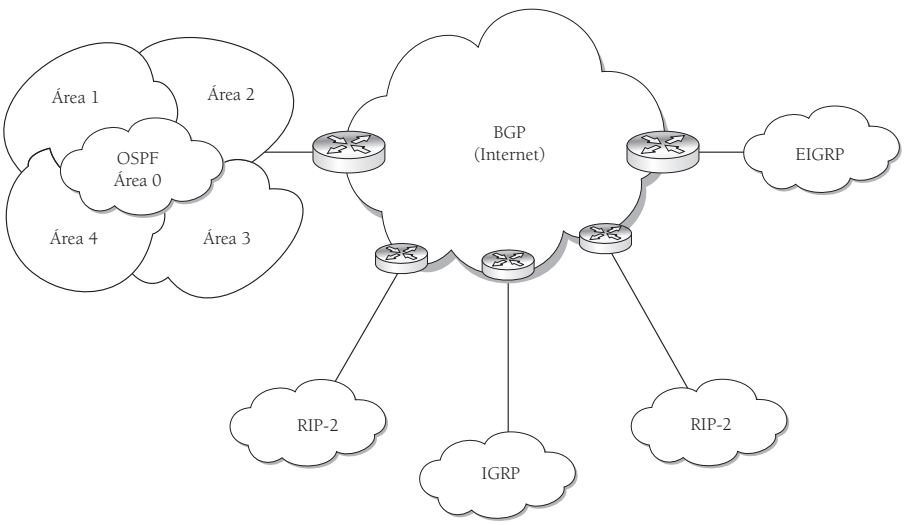


Zona de flujo de transmisión VLAN

Las VLAN dan jerarquía a las redes conmutadas al limitar las transmisiones a grupos discretos de usuarios. Esto combina la velocidad de ancho de banda conmutado con la topología jerárquica que por ahora está disponible sólo en las redes de ancho de banda compartido. Además, la flexibilidad de VLAN asigna a los usuarios a grupos de trabajo lógicos en lugar de tener que agruparlos por dispositivo.

Optimización de ruta

Las interconexiones usan protocolos de control para enrutar mensajes. Demasiado cambio dinámico en las interconexiones (a través del crecimiento, los patrones de tráfico cambiantes, un dispositivo que deja de funcionar, y cosas parecidas) que pueden operar por sí mismos en algún grado al actualizar constantemente las tablas de enrutamiento del dispositivo. Las redes enrutadas dependen de que los protocolos de enrutamiento lleven registro de las rutas a través de las interconexiones. Por ejemplo, muchas interconexiones pequeñas usan RIP 2; casi todas las grandes usan EIGRP u OSPF (EIGRP es propiedad de Cisco; OSPF es un estándar abierto). Intercambian listas de rutas, principalmente dentro de un sistema autónomo, y se usan para conectar segmentos LAN. BGP intercambia listas de sistemas autónomos y se usa para conectarse a Internet.



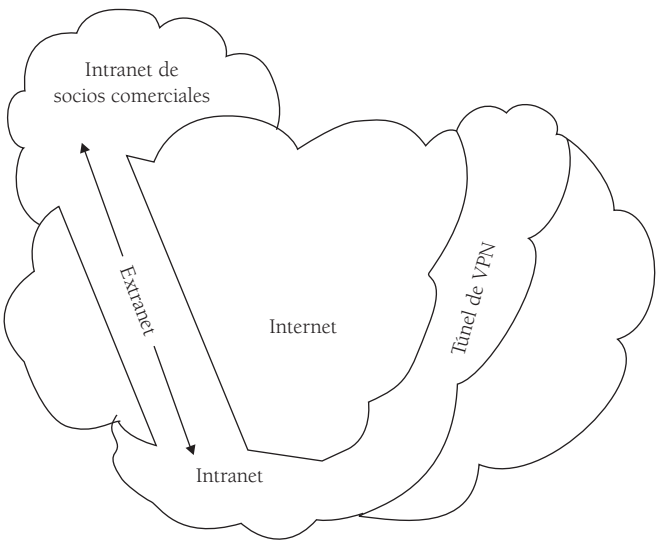
Como ya lo aprendió, las interconexiones mantienen un grado de conciencia propia mediante los protocolos de descubrimiento, que encuentran nuevos dispositivos y mantienen una revisión constante del estado de los conocidos. Esos protocolos, de los que Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco) es un ejemplo, son los actores de reparto en los protocolos de enrutamiento. Cuando tiene lugar un evento, se descubre y la noticia se pasa hasta que la población completa de dispositivos converge en una nueva lista de rutas. En ocasiones aparecen bucles donde una ruta sugerida se voltea hacia su dispositivo de origen, creando rutas no esenciales que pueden hacer más lenta o incluso llevar a que deje de funcionar una interconexión. Los protocolos de enrutamiento usan mediciones para afinar las interconexiones. RIP usa sólo conteo de saltos, pero los protocolos más sofistica-

dos usan varias mediciones que pueden combinarse en una matriz ponderada para dirigir el tráfico hacia los vínculos deseados.

Las redes conmutadas no son tan complejas. Los conmutadores mantienen sólo una lista de direcciones MAC en que la MAC que se usó más recientemente aparece en la parte superior, y la primera siempre será la primera elección. Las redes conmutadas usan el Spanning Tree Protocol (STP, protocolo de árbol extendido) para evitar bucles.

Arquitecturas y aplicaciones de interconexión

En los últimos años, los requisitos de diseño de la empresa típica han cambiado radicalmente. Estos cambios se han presentado en extremos opuestos de la topología. En la parte inferior, la segmentación que usa concentradores con conmutadores de acceso han aumentado enormemente el número de segmentos LAN y, por tanto, la cantidad de tráfico que recorre la espina dorsal entre los segmentos. En la parte superior, arquitecturas de computación completamente nuevas se están volviendo el estándar, con las intranets basadas en Web remplazando los sistemas de administración cliente-servidor tradicionales, las extranets transformando los sistemas de Electronic Data Interchange (EDI, intercambio de datos electrónico) y las Virtual Private Networks (VPN, redes privadas virtuales) reemplazando las Wide Area Networks (WAN, redes de área amplia) de línea arrendada.



Algo que produce unos cambios es el hecho de que las nuevas aplicaciones de red han cambiado las características del tráfico. Por ejemplo, la videoconferencia se está volviendo popular, aumentando la necesidad de configuraciones optimistas para manejar transmisiones múltiples (donde una sola copia de un mensaje se reenvía a un subconjunto de hijos de destino).

El modelo de diseño jerárquico de tres capas

Las topologías jerárquicas son inherentemente mejores que las planas por diversas razones, siendo la principal que la jerarquía contiene tráfico a su área local. La regla general que los

diseñadores deben usar es que el tráfico de transmisiones no debe exceder el 20% de los paquetes que pasan por cada vínculo (la implicación de esto es que la segmentación impulsará de manera natural la velocidad de transmisión de datos al aislar el tráfico a sus usuarios más probables) esta regla se aplica sólo a la cantidad de paquetes transmitidos en la mesa del tráfico, y no debe confundirse con la regla del 80/20. Esta regla establece que el 80% de todo el tráfico permanece en casa y sólo el 20% sale del área local.

Una topología plana (en la que cada dispositivo hace más o menos el mismo trabajo) aumenta el número de vecinos con los que un dispositivo individual debe comunicarse. Esto aumenta de alguna manera la cantidad de tráfico de carga útil que un dispositivo es capaz de transportar y aumenta en gran medida el tráfico. Por ejemplo, cada vez que un enrutador recibe un mensaje de transmisión, su CPU se interrumpe. En el caso de muchas interconexiones pequeñas, una topología plana es suficiente, y el costo añadido y la complejidad que la jerarquía requiere no vale la pena. Pero no se requieren muchos segmentos LAN para dañar el rendimiento y la confiabilidad de una interconexión, con dispositivos y hosts dando lugar a un tráfico innecesario.

Por esto es que la industria se adhiere a un modelo de diseño jerárquico clásico. El modelo tiene tres capas: la de acceso de distribución y central. Esto separa el tráfico local del tráfico de alto volumen que pasa entre los segmentos LAN y las áreas, y permite a los dispositivos de red en cada capa concentrarse en hacer su trabajo específico. El modelo jerárquico se describe en la figura 14-1.

La jerarquía es posible mediante la segmentación (la práctica de dividir hosts en segmentos LAN más pequeños). Hace 50 años, casi todos los segmentos hosts eran en realidad cables que recorrían paredes y techos falsos. Hoy en día, casi todos están formados por concentradores de cables y conmutadores de acceso. La segmentación y la topología jerárquica arrojan varios beneficios:

- ▼ **Rendimiento** El tráfico se aísla en las áreas de origen, con lo que se estrechan los dominios de colisión de paquetes Ethernet y se acelera la velocidad de transmisión de datos.
- ■ **Confiabilidad** Casi todas las fallas se aíslan a un segmento en que se originó el problema.
- ■ **Simplicidad** Al separar áreas diferentes, los elementos de red pueden replicarse de acuerdo con las necesidades en toda la interconexión.
- ■ **Escalabilidad** Los elementos de diseño modular pueden agregarse a medida que la interconexión crece con el tiempo, con cambios mínimos a las redes existentes.
- ▲ **Seguridad** El acceso puede controlarse en uniones bien definidas entre las capas.

De manera natural a las interconexiones tienden a una jerarquía de dos niveles. Los concentradores y los conmutadores se conectan a dispositivos host en segmentos LAN, y la espina dorsal conecta los segmentos en una red local, sin importar si se encuentra dentro de un piso, un edificio, un campus de oficinas o aun un área metropolitana. Ésta es una topología relativamente plana en el sentido de que, a pesar de que los dominios de colisión están limitados, el tráfico excesivo de la trasmisión aún devora parte del ancho de banda disponible. Esto hace que la capa de distribución sea la clave. Al aislar el tráfico, la capa de distribución también aísla los problemas y la complejidad.

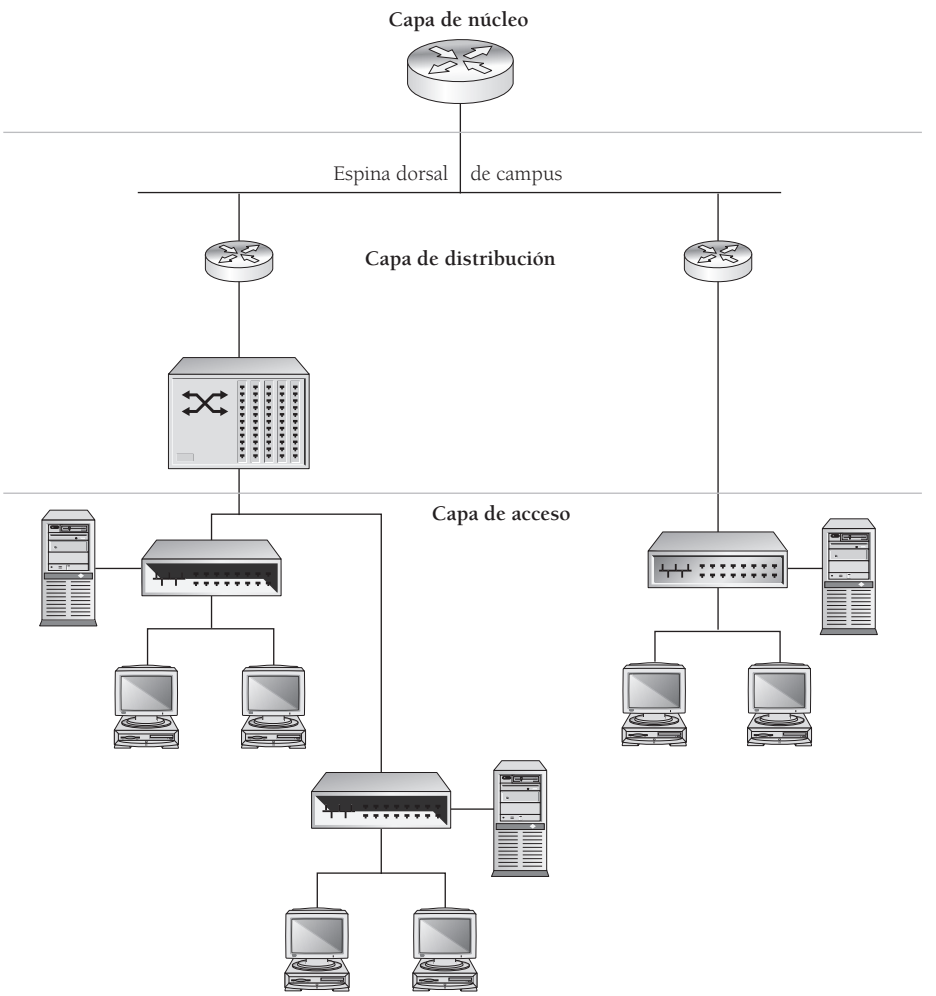


Figura 14-1. La topología jerárquica clásica de tres capas se basa en la segmentación.

La jerarquía también ayuda a reducir costos. Al dividir hosts y tráfico, las variaciones están limitadas a menos segmentos LAN, e incluso un solo segmento. Entre las variaciones incluyen cosas como protocolos de escritorio (IP, IPX, AppleTalk), volúmenes de tráfico (grupos de trabajo en comparación con espina dorsal) y tipo de tráfico (grandes archivos gráficos, correo electrónico, HTTP). La jerarquía permite a los diseñadores de red afinar la configuración para un trabajo particular que tienen a mano. Se hacen ajustes en el modelo del dispositivo de red comprado y en la manera en que está configurado en cuanto a la memoria, los módulos, el software y la configuración de los parámetros del archivo config.

La capa de acceso

La capa de acceso está integrada principalmente por concentradores y conmutadores, que sirven para segmentar los dispositivos host, como PC y servidores, en muchos segmentos LAN integrados por ancho de banda compartido o conmutado. Aquí es donde tiene lugar el filtro de la capa MAC.

Si una interconexión tiene sitios remotos, como sucursales u oficinas centrales, la capa de acceso también incluye servidores de acceso y enrutadores de acceso. Las WAN deben usar algún tipo de medio de transmisión a larga distancia. Ahora hay una amplia selección de medios, como líneas digitales T1 y T3 y las redes digitales públicas Frame Relay. Los usuarios remotos del mercado telefónico emplean línea de módems análogas y, en ciertas áreas, tecnologías de ancho de banda más elevado, como Digital Suscriber Line (DSL, línea de suscriptor digital) e Integrated Services Digital Network (ISDN, red digital de servicios integrados). En la figura 14-2 se muestra una funcionalidad de la capa de acceso.

En redes grandes, la capa de acceso puede incluir enrutadores. Estos enrutadores internos sirven principalmente para aislar el exceso de carga, controlar el tráfico y mejorar la seguridad interna. La capa de acceso abarca una mezcla de tecnologías en casi todas las interconecciones. Dial-on-Demand Routing (DDR, enrutamiento de marcado bajo pedido) se ha vuelto popular para conexiones remotas, porque mantiene un vínculo inactivo con excepción de los momentos en que el tráfico está por enviarse, con lo que reduce los costos de las telecomunicaciones.

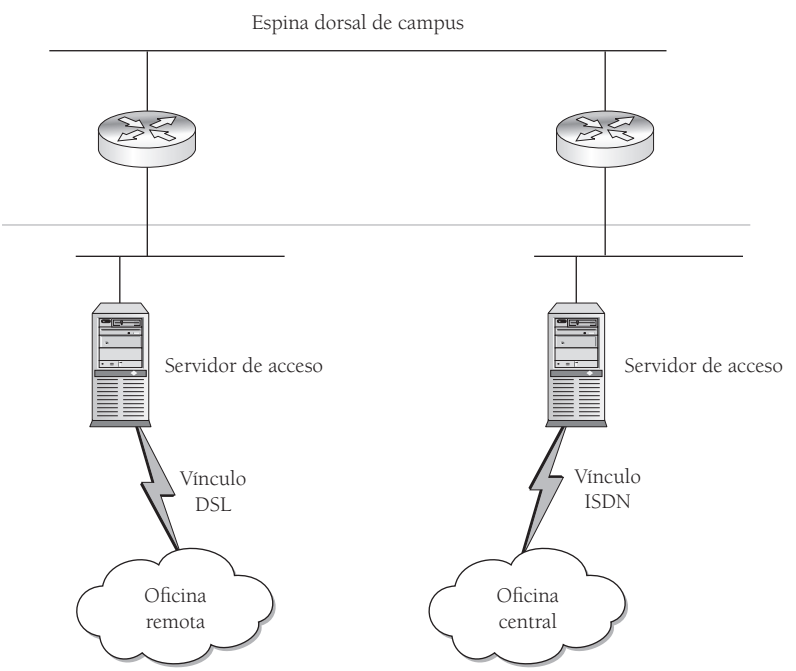


Figura 14-2. La capa de acceso proporciona conectividad local y remota a los hosts.

Muchas de las empresas tienen tecnologías heredadas que gradualmente se van desplazando a medida que se implementan nuevas. Por ejemplo, muchas compañías grandes aún utilizan WAN T1 de línea arrendada junto con VPN en crecimiento, sustituyendo el uso de red compartida para líneas arrendadas dedicadas. Desde un punto de vista táctico, esto es necesario porque los enrutadores deben actualizarse junto con cada vínculo de VPN.

La capa de distribución

La capa de distribución está integrada principalmente por enrutadores y conmutadores de capa 3. Se utilizan para separar el tráfico local lento de la espina dorsal de alta velocidad. El tráfico en la capa de acceso tiende a requerir una gran cantidad de ancho de banda porque allí es donde reside la mayor cantidad de LAN y direcciones de host. El tráfico excesivo de protocolos de red para protocolos de descubrimiento, SNMP, protocolos de enrutamiento y otros sistemas de control de redes es más pesado en la capa de acceso.

Debido a que los enrutadores son lo suficientemente inteligentes para leer la dirección de red y examinar los paquetes, también mejoran el desempeño al enviar el tráfico de la manera más directa posible a su destino. Por ejemplo, los enrutadores de la capa de distribución definen la trasmisión y los dominios de trasmisión múltiple a través de los segmentos LAN. Los dominios están, como opción predeterminada, limitados a segmentos LAN; los enrutadores pueden extender los dominios entre segmentos como lo determina el diseño de la jerarquía. En la figura 14-3 se describe una funcionalidad de capa de distribución.

En configuraciones que usan conmutadores de varias capas, los dispositivos de la capa de distribución enrutan los mensajes entre VLAN. La **conmutación de varias capas** es una tecnología en que los paquetes se filtran y se reenvían con base en las direcciones de MAC y de red. El Catalyst 6500 es quizás el mejor ejemplo de un conmutador de varias capas, incorporando la Multilayer Switch Feature Card (MSFC2, tarjeta de características de conmutador de varias capas) además de los que tienen electrónica típica de conmutador.

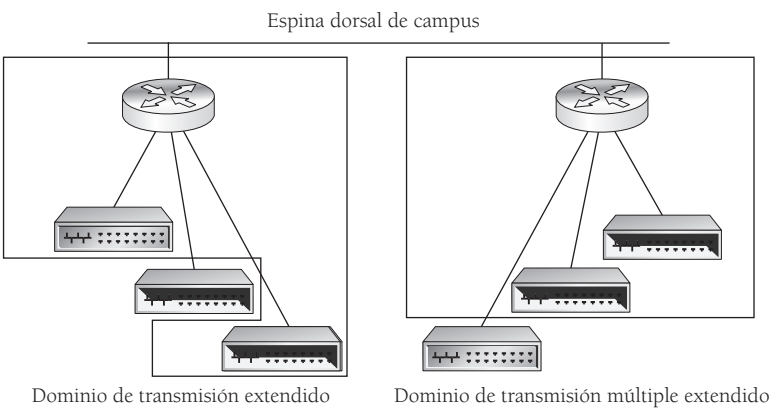


Figura 14-3. La capa de distribución es la clave para proporcionar una jerarquía funcional.

Casi todos los servicios de valor agregado se proporcionan mediante dispositivos en la capa de distribución. La traducción de direcciones tiene lugar en esta capa, por lo general en un enrutador de gateway o un firewall (en si mismo, un tipo de enrutador). La agregación de direcciones también tiene lugar aquí, además de una generación de área si la interconexión está ejecutando dominios de enrutamiento SDPF. Otros servicios también se realizan en los enrutadores de capa de distribución: la traducción entre protocolos como IPX e IP, cifrado entunelamiento VPN; seguridad basada en tráfico usando listas de acceso y algoritmos de firewall basada en el contexto; y seguridad basada en el usuario que emplea protocolos de seguridad como RADIUS, TACACS+ y Kerberos.

La capa de núcleo

La capa de núcleo es la capa de la espina dorsal. En interconexiones grandes, el núcleo incorpora varias espinas dorsales, desde LAN de espina dorsal de campo hasta las regionales. En ocasiones, las LAN especiales de espina dorsal se configuran para manejar un protocolo específico o trágico particularmente sensible. Casi todas las espinas dorsales existen para conectar segmentos LAN, por lo general las que se encuentren dentro de un edificio particular o un campus de oficinas. En la figura 14-4 se describe la manera en que la capa de núcleo se vería en una interconexión típica de una empresa grande.

Para ejecutarse rápidamente, una LAN de espina dorsal debe configurarse para experimentar un mínimo de interrupciones. El objetivo es tener la mayor cantidad posible de los ciclos de CPU del dispositivo espina dorsal dedicados a transferir paquetes entre segmentos. La capa de distribución permite esto al conectar segmentos LAN de grupo de trabajo y proporcionar servicios de enrutamiento de valor agregado. Un mínimo de manipulación de paquetes debe ocurrir en este nivel. Por esto casi todas las nuevas espinas dorsales son LAN conmutadas. La necesidad de interpretación de direcciones en el núcleo se minimiza mediante el procesamiento ya realizado por los enrutadores de la capa de distribución, así que ¿por qué no usar tecnología de conmutación para mover datos en la espina dorsal de manera más rápida?

ATM (Asynchronous Transfer Mode, modo de transferencia asincrónico) y Gigabyt Ethernet lucharon para convertirse en la tecnología de espina dorsal conmutada preferida. ATM tenía un elemento de ventaja en el caso de las aplicaciones multimedia porque usan celdas de tamaño fijo en lugar de paquetes de longitud variable de Ethernet. La ventaja obvia de las espinas dorsales conmutadas de Gigabyt Ethernet es la compatibilidad más fácil con los millones de LAN Ethernet que ya están instalados en todo el mundo. Sin embargo, al final Gigabyte Ethernet ganó la guerra.

ATM es un estándar internacional de retrasmisión de celdas para tipos de servicio como video, voz y datos. Las celdas de longitud fija de 53 bytes aceleran la transferencia de datos al permitir que el procesamiento ocurra en el hardware. Aunque los productos ATM están allí para que los datos recorran todo el camino hasta el escritorio, la tecnología está optimizada para trabajar con medios de transmisión de alta velocidad como OC-48 (2.5 Gbps), T3 (45 Mbps) y la contraparte europea de T3, E3 (34 Mbps).

Métodos de diseño

Con los años, la industria de las interconexiones ha desarrollado un conjunto de conceptos y mejores prácticas para el uso en el diseño de las interconexiones. Casi todas las interconexio-

nes están en evolución; muy pocas se han diseñado a partir de una hoja en blanco de papel. A medida que las topologías de interconexión evolucionan con el tiempo y las circunstancias, es más difícil mantener un diseño de red jerárquico riguroso (sobre todo en empresas grandes con estructuras de administración distribuida o en tiendas que tienen alta rotación de personal en sus equipos de red).

Redundancia y equilibrio de carga

Redundancia es la práctica de configurar el equipo de copia de seguridad. Esto se hace para proporcionar tolerancia a fallas, donde el tráfico se desplazará al dispositivo de copia de

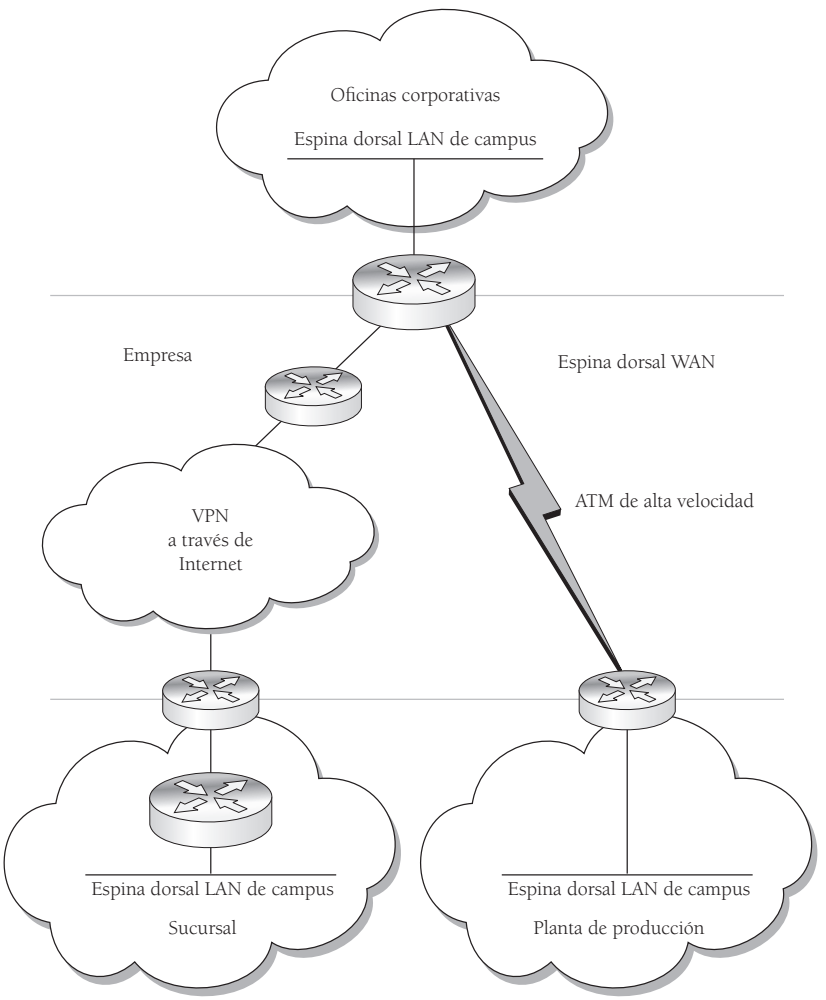
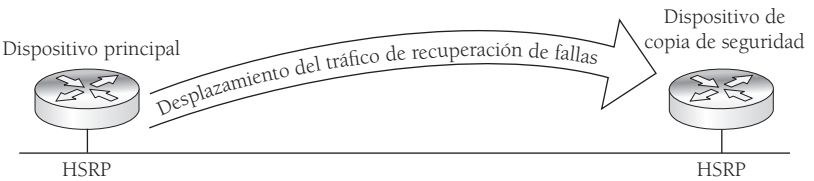


Figura 14-4. La capa de núcleo incluye espinas dorsales de LAN de campus y espinas dorsales de WAN.

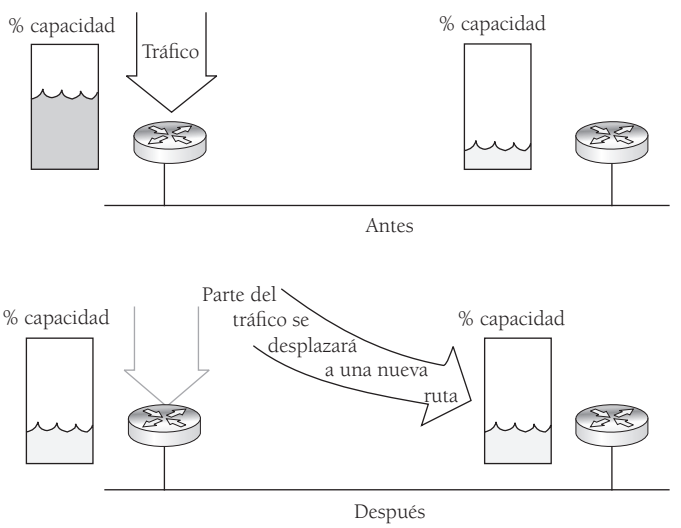
seguridad si falla la unidad principal, proceso al que se le denomina recuperación de fallas. Por ejemplo, casi todas las espinas dorsales de alta velocidad tienen conmutadores duales configurados en cada extremo en caso de que el conmutador principal falle. Otra salvaguarda común es tener suministros de poder redundantes dentro del dispositivo, de modo que si uno falla, el dispositivo siga funcionando.



La tecnología de Cisco que soporta la redundancia es el Hot Standby Router Protocol (HSRP, protocolo de enrutador activo en espera), un conjunto de comandos en IOS. *Activo en espera* es un término de la industria de la computación que significa que la unidad de copia de seguridad está siempre activa ejecutándose, lo que permite la recuperación de fallas automáticas en caso de una falla. HSRP funciona al crear un grupo de enrutadores donde se elige uno como el enrutador activo y otro como el que está en espera, un enrutador "fantasma". Todos comparten una dirección IP y NAC virtual a la que servirá el enrutador activo. Este es monitoreado por otros en el grupo, y en caso de que falle, el enrutador en espera toma el control del tráfico procesando las tareas, y otro enrutador de copia de seguridad (si hay más de dos) será elegido como el nuevo enrutador en espera. Las recuperaciones de fallas se logran sin intervención del ser humano y por lo general se realizan en unos cuantos segundos.

Debido a que las configuraciones redundantes son costosas, las configuraciones tolerantes a fallas suelen estar limitadas a dispositivos críticos. La redundancia se configura de manera más común en dispositivos de espina dorsal y firewalls, donde la falla del dispositivo tendría el efecto más amplio en la red general.

Equilibrio de carga es una técnica de configuración que desplaza el tráfico a un vínculo alterno si un cierto umbral se excede en el vínculo primario. El equilibrio de carga puede



lograrse a través de varios medios, como afinar las mediciones de enrutamiento en los archivos config del enrutador dentro de los dominios de protocolo de enrutamiento.

El equilibrio de carga es similar a la redundancia porque un evento hace que el tráfico cambie de dirección, y debe estar presente el equipo interno a la configuración. Pero en el equilibrio de carga, el equipo alterno no es necesariamente equipo redundante que sólo opera en el caso de falla.

Topología de mallas

Un buen diseño incorporará una topología de mallas para lograr la redundancia y el equilibrio de carga. Una malla en donde los dispositivos de red (por lo general enrutadores o conmutadores) están conectados directamente. En una topología de malla completa, todos los nodos de la red tienen circuitos físicos o virtuales conectando cada nodo de la interconexión. También tiene una topología de malla parcial, en que algunas partes de la topología pertenecen completamente a la malla pero algunos nodos están conectados sólo a uno o dos nodos adicionales. En la figura 14-5 se describen las dos.

A primera vista, todas las mallas parecen ser algo inherentemente bueno. Al observar el ejemplo de la figura 14-5, puede ver fácilmente los beneficios de la topología de malla completa:

- ▼ **Rendimiento** Es sólo un salto a cualquier red conectada a uno de los otros enrutadores, y cuanto menor sea la cantidad de saltos, mayor será la velocidad.
- ■ **Disponibilidad** Tener rutas redundantes significa que si un enrutador deja de funcionar, uno o más enrutadores alternos siempre están disponibles.
- ▲ **Equilibrio de carga** Las rutas alternas también pueden usarse para operaciones normales, donde los parámetros de enrutamiento pueden configurarse para usar rutas alternas si una carga de tráfico presente se excede en el enrutador principal.

La interconexión parcialmente incluida en la malla de la parte inferior de la figura 14-5 no tiene estas ventajas. Por ejemplo, para ir del enrutador A al C se requieren dos saltos de enrutador, no uno. Si los enrutadores que se encuentran en ambos lados del enrutador F dejan de funcionar, no podrá comunicarse con el resto de la interconexión. Además, menores conexiones de malla reducen las oportunidades del equilibrio de carga. Sin embargo, aunque el enmallado puede tener beneficios, debe usarse con cuidado, porque tiene los siguientes costos:

- ▼ **Costo económico** Cada interfaz de enrutador (o conmutador) dedicado a una malla no puede usarse para conectar un segmento LAN. El enmallado consume capacidad de hardware.
- ■ **Exceso de tráfico** Los dispositivos anuncian constantemente sus servicios entre sí. Cuantos más vínculos de malla tenga un dispositivo, más paquetes de anuncios transmitirá, con lo que consumirá ancho de banda de carga útil.
- ■ **Vulnerabilidad** Los enmallados hacen más difícil contener problemas dentro de un área local. Si, por ejemplo, un dispositivo mal configurado empieza a propagar mensajes de transmisión indiscriminados, cada elemento de una malla causará que la tormenta de transmisión se irradie mucho más allá del origen.
- ▲ **Complejidad** Las conexiones adicionales dificultan aislar los problemas. Por ejemplo, sería más difícil llevar registro del dispositivo que causa la tormenta de transmisiones en una interconexión con una malla completa o pesada, porque habría muchos rastros que seguir.

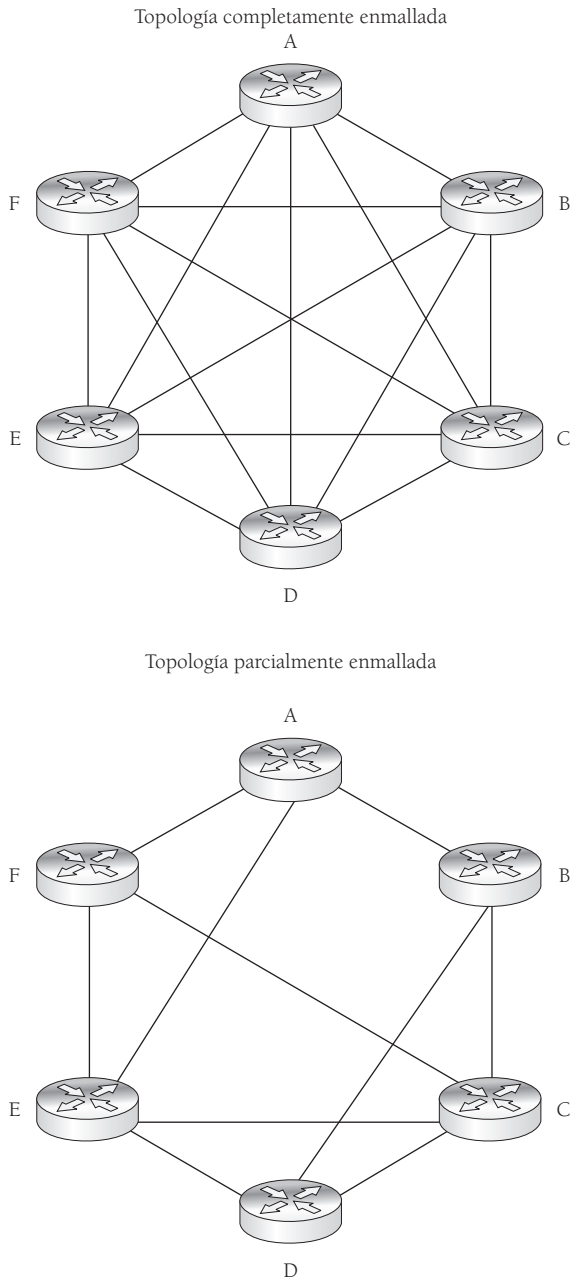


Figura 14-5. Cada una de las topologías enmalladas de manera completa y parcial tiene sus pros y sus contras.

Por estas razones, pocas interconexiones están completamente enmalladas. La práctica general es enmallar completamente la parte de la espina dorsal de las topologías para proporcionar tolerancia a fallas y equilibrio de carga a lo largo de estos vínculos críticos, pero sólo enmalla parcialmente el acceso y las topologías de la capa de distribución.

Configuraciones de puertas traseras y cadena

En ocasiones las circunstancias determinan la desviación de un modelo jerárquico estricto. Las dos desviaciones comunes de la topología se denominan puerta trasera y cadenas. Una *puerta trasera* es cualquier conexión dirigida entre dispositivos en la misma capa, por lo general la capa de acceso. Una *cadena* es la visión de una o más capas debajo de la capa de acceso. En la figura 14-6 se describen las dos.

En ocasiones, tiene sentido configurar una puerta trasera. Por ejemplo, tal vez quiera vincular directamente los sitios remotos si los vínculos a los enrutadores de la capa de distribución son costosos o lentos. Las puertas traseras también proporcionan un grado de redundancia: si el vínculo de la puerta trasera deja de funcionar, los dos sitios remotos pueden servir para recuperar de la falla al enrutador de la capa de distribución y mantener la comunicación. Sin embargo lo más frecuente es que surjan puertas traseras y cadenas debido a la mala planeación de red o un administrador revelado que instala equipo de red sin participar en el equipo de red.

DISEÑO PARA SATISFACER LAS NECESIDADES

Le sorprenderá saber cuántas interconexiones (incluso grandes y sofisticadas) han crecido de manera azarosa. El crecimiento de la red sin administración ocurre por diversas razones. La más común es que las cosas simplemente suceden demasiado rápido. Tenga en cuenta que las realidades que ahora damos como hechos (computación cliente-servidor, intranets, Web, extranets), eran sólo conceptos hace menos de una década. Esto dejó a muchos admi-

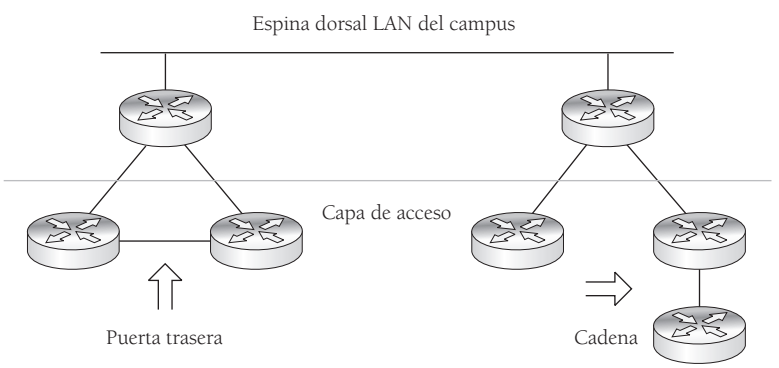
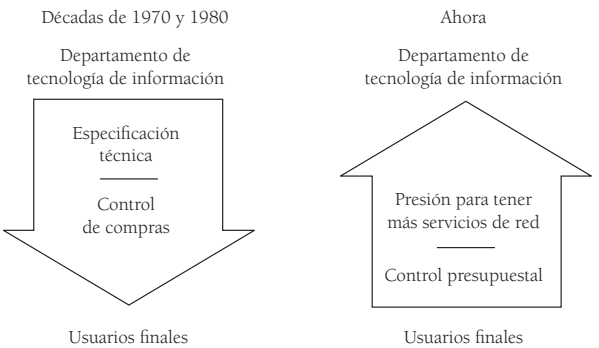


Figura 14-6. Las puertas traseras y las cadenas violan la topología jerárquica de tres capas.

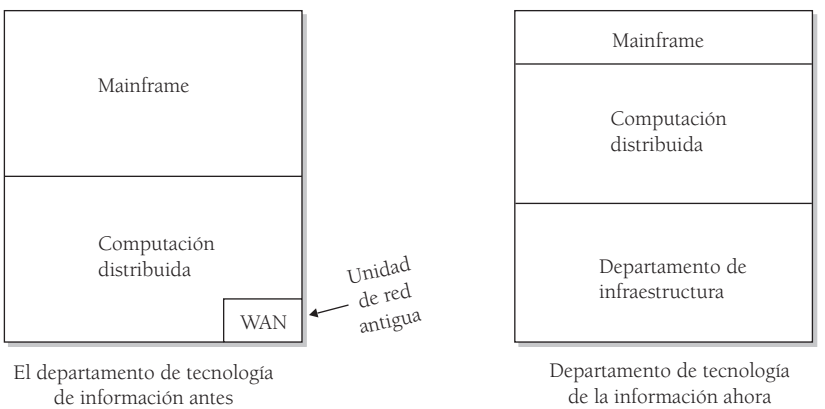
nistradores de tecnología de información sin prepararse para formular planes de red estratégicos, bien investigados y razonados para sus empresas.

En muchos casos, un plan no habría servido de mucho. El entusiasmo de la administración va y viene, pero algo que arruine las cosas y la frase "si yo pago, tengo la palabra". La tendencia de la administración ha sido hacia aprender las estructuras organizacionales, con capas mínimas entre el presidente y el trabajador. Casi todos los departamentos de tecnología de información ahora son "presupuestados" por divisiones individuales, grupos o incluso departamentos. En otras palabras, las decisiones de la tecnología prima de la información cada vez se hacen con más frecuencia de abajo hacia arriba y las toma la entidad que tiene el presupuesto, no el departamento central de tecnología de información.



Este tipo de toma de decisiones distribuida se ha magnificado por la lentitud de muchos departamentos de tecnología de información para responder a las demandas emergentes del cliente orientadas por cosas como reingeniería de procesos de negocios, fusiones, adquisiciones y cooperativas de socios comerciales. De modo que hemos llegado al punto en que muchos administradores de usuarios finales simplemente tiran la arquitectura técnica corporativa, levantan el teléfono y ordenan nuevas redes por cuenta propia.

La tendencia en los últimos años ha sido que los departamentos de tecnología de la información dividan las redes en un grupo separado llamado *infraestructura* (separan las cabezas del chip de las cabezas del cable por decirlo así). Esto se hace porque las interconexiones simplemente se han vuelto demasiado grandes y complicadas como para dejarlo a un



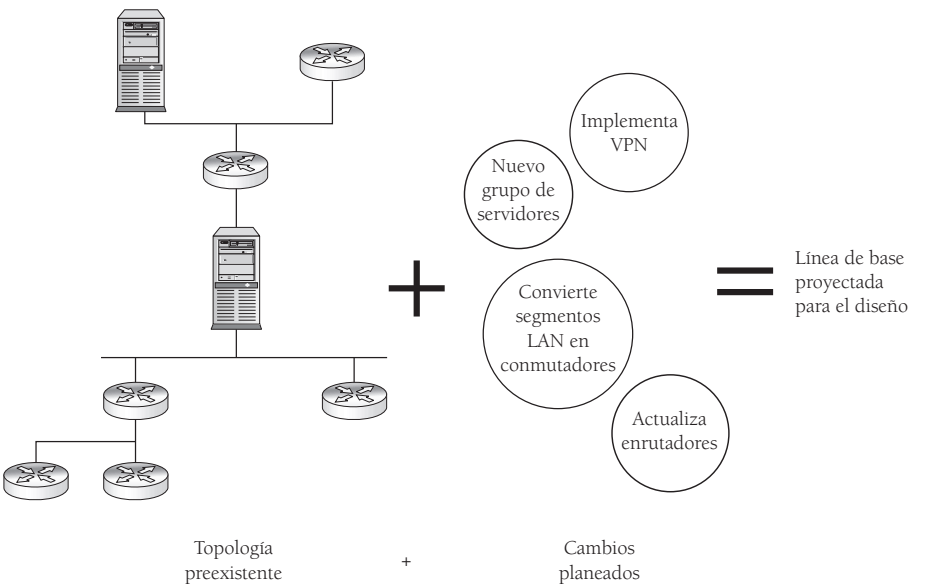
administrador que, digamos, tiene antecedentes en COBOL y administración de proyectos de software de mainframe. Las redes tienen ahora sus propias reglas. Se está convirtiendo rápidamente en una disciplina propia con un conjunto propio de mejores prácticas (algunas de las cuales revisaremos en el resto de este capítulo).

Se han desarrollado tecnologías que ayudan a controlar la planeación de las redes. No es de sorprender que esto tenga un fuerte parecido con las metodologías de procesamiento de datos. Lo primero y más importante por supuesto es adecuar la solución a las necesidades de negocio a través de alguna forma de evaluación de necesidades (tanto presentes como futuras).

Comprensión de las redes existentes

Como ya se mencionó, pocos diseños de red empiezan desde cero. Aunque sería estupendo trabajar a partir de una hoja de papel en blanco, casi todos los diseños deben acomodarse a una red preexistente. La mayor parte de ellas son diseños incrementales para servir a más usuarios o actualizar la capacidad de ancho de banda, o ambos. Por ejemplo, una actualización común es insertar una capa de enrutadores entre la espina dorsal LAN y la capa en que los hosts acceden la red. Esto se está haciendo en muchas empresas para mejorar el rendimiento y acomodar el crecimiento proyectado. Cualquiera que sea el cambio, la infraestructura existente debe analizarse por completo antes de siquiera considerar una compra.

En la siguiente sección se describen los métodos para la planeación y diseño de redes. Se concentran en establecer una línea de base sobre el aspecto que tendrá la red después de la implementación. Como actualización sobre temas, una línea de base es un punto de partida de la red, expresado en volúmenes de tráfico, flujos y características. Se crean estimados de márgenes de error y crecimiento proyectado por arriba y por abajo de la línea de base.



Cuando se diseña un área de red completamente nueva, debe llegar a una línea de base de diseño a partir de suposiciones bien investigadas, a menudo derivadas del papeleo o de

otro tráfico de datos que no pasa por la red, y que ya está en el lugar. Si una topología de red existente se está actualizando, la línea de base se toma al medir sus características. Si el escenario de diseño abarca elementos que están y que no están en la red, entonces los dos se deben compilar juntos. Cualquiera que sea el caso, los principios y métodos de un buen diseño de redes siguen siendo los mismos.

Caracterización de las redes

Existen varios métodos para comprender una interconexión lo suficientemente bien como para formular un diseño apropiado. Estos métodos se aplican a una interconexión existente o una topología que habrá de construirse desde cero. Como esperaría, los métodos se concentran en la geografía y en el tráfico (en otras palabras, donde se encuentran los nodos de la red y lo que viaja entre ellos). Un nodo de red es cualquier dispositivo de la topología (incluidos dispositivos de red, como enrutadores, y hosts de carga útil, como servidores). Para nuestros propósitos, cuando se diseñe una red desde cero, un nodo podría ser una entidad no relacionada con una computadora como un escritorio o un gabinete de archivos. Lo importante es identificar dónde están los usuarios y qué están usando.

Calidad del servicio

La caracterización de las redes es buena para administrar y para diseñar. La industria está impulsando el concepto de Quality of Service (QoS, calidad del servicio), que es un método que se basa en gran medida en la caracterización del tráfico. QoS es la técnica para asegurar la velocidad de transferencia de datos para el tráfico a través de una interconexión. Es más sofisticado que sólo garantizar que ciertos vínculos se ejecutarán en cierto nivel de transmisión de datos. Casi todo el aseguramiento de la calidad de servicio está relacionado con un tipo particular de tráfico, digamos, priorizar las transmisiones múltiples de video para aprendizaje a distancia mediante correo electrónico y otros medios menos críticos para el tráfico.

Como imaginará, la implementación de la directiva de QoS depende en gran medida de la información reunida a través de SNMP y RMON y presentada a través de consolas NMS, como Resource Manager Essential y Campus Manager. Como esas aplicaciones de consola, QoS usa el modelo cliente-servidor al almacenar una base de datos de QoS, e implementa directivas a través de applets construidas con un propósito, como QoS Policy Manager, QoS Distribution Manager y Cisco Assure.

QoS Policy Manager de Cisco crea comandos abstractos que agrupan comandos IOS individuales para realizar una tarea a partir de la GUI Cisco Policy Manager. Al igual que con otras applets de consola de NMS, cuando oprime un botón, se aplican uno o más comandos en el dispositivo de red del cliente que se está configurando. Algunos subcomandos de QoS son genéricos de IOS (el comando **interface**, por ejemplo); otros son específicos de QoS. Los principales comandos abstracos de QoS son los siguientes:

- **WFQ** *Weighted Fair Queuing* (*disposición en cola justa y ponderada*). Combina los comandos **interface** y **fair-queue** para que los administradores de red asignen prioridades a la manera en que una mezcla de tipos de tráfico fluirán a través de ciertas áreas de la topología. Por ejemplo, al correo electrónico podría dársele una mayor prioridad en servidores de Lotus Notes, pero no en otro lugar.
- **WRED** *Weighted Random Early Detection* (*detección aleatoria temprana ponderada*). Combina los comandos **interface** y **random-detect**. (El comando **random-detect**

acepta un valor ponderado para representar la importancia relativa del tipo de tráfico.) WRED trata de controlar la congestión de tráfico a medida que empieza a emerger.

- **CAR** *Committed Access Rate* (*de acceso comprometido*). Es la tecnología de control de ancho de banda QoS. Usa un MIB ROM sofisticado para reconocer los tipos de tráfico, establece prioridades y limita las velocidades de paquete conforme sea necesario.

Las técnicas de QoS se aplican principalmente en el nivel de la interfaz de red, y hace un uso pesado de las listas de control de acceso para filtrar paquetes. La idea es diferenciar los tipos de tráfico dentro de las áreas de la topología e influir en el comportamiento de la red (una técnica denominada *moldeado del tráfico*). El objetivo del moldeado del tráfico es garantizar niveles mínimos de servicios de extremo a extremo para varios tipos de tráfico.

Comprensión del flujo del tráfico

La compresión y documentación del flujo del tráfico es el primer paso en el diseño de la red. Dibujar una analogía con el diseño de una supercarretera parecería demasiado obvio, pero los dos son notablemente similares. El diseñador de caminos debe saber dónde debe estar el camino, qué ancho debe tener, qué tipo de superficie no debe cubrir y qué tipo de reglas de control del tráfico no habrán de aplicarse. Todo esto son en gran medida funciones del flujo del tráfico.

Las características del tráfico son, en gran medida, asunto de dirección, simetría, tamaños de paquetes y volumen. Un flujo unidireccional hace casi todo comunicándose en una dirección; un flujo bidireccional se comunica casi con la misma frecuencia en ambas direcciones de la colección. Un flujo asimétrico envía más datos en una dirección que la otra; un flujo simétrico envía casi iguales cantidades de flujo hacia delante y hacia atrás. Por ejemplo un flujo de una sesión HTTP es bidireccional y asimétrico porque una gran cantidad de mensajes se envían en ambas vías, pero los datos se descargan principalmente del servidor Web al cliente del navegador.

Identificación de las fuentes de tráfico Para comprender el flujo del tráfico, debe conocer sus orígenes. Esto se hace al identificar grupos de usuarios, no personas individuales. En la terminología de la metodología de la computación, un grupo de usuarios a menudo se denomina una *comunidad* (tal vez debido a que el término obvio, *grupo de usuarios*, ya se usa para asociaciones de clientes, como el Cisco User Group).

Debe reunirse un inventario de características de alto nivel, como la ubicación y las aplicaciones usadas. Eso no quiere decir que debería uno salir con un portapapeles reuniendo información. La mayoría de los diseñadores de red obtendrían esta información de una base de datos de herramientas como Resource Manager Essentials o Campus Manager. En el siguiente ejemplo se muestra una forma que podría usarse para reunir información del usuario:

Comunidad	Número de personas	Ubicaciones	Aplicaciones	Tipo de host
Contabilidad	27	San Luis	AR, AP, GL	AS/400
Servicio al cliente	200	México, DF	Call Center	Windows NT 4.0

Reunir cualquier tipo de información que quiera. Por ejemplo, tal vez no quiera documentar el tipo de host que el grupo usa si todos tienen una PC Pentium. Por otra parte, si hay una mezcla de terminales "tontas", clientes delgados, PC y estaciones de trabajo Unix y Linux, tal vez quiera saber quién tiene qué. Esta información le ayudará a calcular de manera más exacta las carreras de tráfico.

Si está analizando una red existente, esta información puede reunirse al activar la opción de registro record-route en IOS. Esta información también puede reunirse utilizando Resource Manager Essentials o Campus Manager.

Identificación de los orígenes de datos y los depósitos de datos Cada empresa tiene usuarios importantes de información. Los expertos identifican a estos usuarios de datos pesados como *depósitos de datos* porque es útil hacer un rastreo hacia los orígenes de datos que usan para ayudar a identificar los patrones del tráfico. Los orígenes de datos más comunes son los servidores de bases de datos, los grupos de discos, las bibliotecas de cintas o de CD, los sistemas inventario, los catálogos en línea, etcétera. Los depósitos de datos suelen ser usuarios finales, pero a veces los servidores pueden serlo. En la siguiente ilustración se muestra información que debe reunirse sobre depósitos de datos.

Depósitos de datos	Ubicaciones	Aplicaciones	Comunidades de usuarios
Grupo de servidores 3	San Luis	AR, AP, GL	Contabilidad
CCSRV	Puebla	Call Center	Servicio al cliente

Documentar cuáles comunidades usan qué depósito de datos le permite correlacionar el tráfico. Ahora puede empezar a conectar hosts de escritorio del usuario con servidores de depósito de datos. Combinar la información de las dos ilustraciones anteriores le permite empezar a dibujar líneas entre cliente y servidor. Correlacione cada comunidad y usuarios con cada depósito de datos, y un perfil exacto de la topología ideal de la red empieza a surgir.

Identificación de las cargas de aplicaciones y los tipos de tráfico Casi todas las aplicaciones de red generan tráfico con características específicas. Por ejemplo, FTP genera tráfico unidireccional y asimétrico relacionado con archivos grandes. En la tabla 14-1 se muestra

Tipo de mensaje	Tamaño aproximado
Página Web	50 KB
Pantalla gráfica de la computadora (como una pantalla de Microsoft Windows)	500 KB
Correo electrónico	10 KB
Documento de procesamiento de palabras	100 KB
Hoja de cálculo	200 KB
Pantalla de terminal	5 KB
Objeto de multimedia (como una videoconferencia)	100 KB
Copia de respaldo de base de datos	1 MB y más

Tabla 14-1. Tamaños y tipos comunes de mensajes.

un ejemplo de tipos de los mensajes comunes y sus tamaños aproximados. Obviamente, los tamaños pueden variar en gran medida, pero se trata de reglas de la industria útiles para estimar cargas de tráfico.

Más allá de la carga de tráfico, es útil conocer el tipo de tráfico. El tipo de tráfico caracteriza a los tipos de dispositivos conectados y la manera en que el tráfico fluye entre ellos:

- ▼ **Cliente-servidor** Por lo general una PC que habla a un servidor Unix/Linux o Windows, se trata de una configuración estándar al día. En los tipos cliente-servidor, el tráfico suele ser bidireccional y asimétrico.
- ■ **Servidor a servidor** Entre los ejemplos se incluyen reflejos de datos a un servidor redundante que sirve como respaldo a otro servidor, servicios de directorio de nombres, etcétera. Este tipo de tráfico es bidireccional, pero la simetría depende de la aplicación.
- ■ **Terminal-host** Muchas aplicaciones basadas en terminal se ejecutan en IP, incluso las conexiones de terminal de IBM a mainframes. Otro ejemplo es Telnet, el tráfico de terminal es bidireccional, pero la simetría depende de la aplicación.
- ▲ **Igual a igual** Entre los ejemplos se incluyen videoconferencia y configuración de PC para acceder a recursos en otras PC, como impresoras y datos. Este tipo de tráfico es bidireccional y simétrico.

La comprensión del tipo de tráfico que pasa por varios vínculos con soy una imagen de la manera de configurarlo. En la siguiente ilustración se muestra información empleada para identificar y caracterizar los tipos de tráfico.

Aplicación	Tipo de tráfico	Comunidad de usuarios	Depósitos de datos	Ancho de banda requerido	Directiva de QoS
Navegador Web	Cliente-servidor	Ventas	Servidor de ventas	350 Kbps	CAR
TN3270	Terminal	Compras	AS/400	200 Kbps	WRED

Frecuentemente, un vínculo está dominado por uno o dos tipos de tráfico. La columna ancho de banda requerido, de la ilustración anterior, se expresa usualmente como un estimado de bits por segundo y podría ser Mbps o incluso Gbps. Una vez que todas las aplicaciones de la interconexión estén identificadas y caracterizadas, el diseñador tiene una línea de base a partir de la cual toma decisiones de configuración pendientes del volumen. El tipo de tráfico resulta especialmente útil para saber dónde y cómo establecer directivas de QoS. En otras palabras, debe identificar cuáles aplicaciones pasaron por un enrutador antes de que establezca apropiadamente los parámetros de QoS en su archivo config.

Comprensión de la carga de tráfico

Después de que se han documentado y caracterizado las comunidades de usuarios, los depósitos de datos y orígenes, y los flujos de tráfico, puede asignarse a un tamaño más adecuado a los vínculos individuales. La información del flujo de tráfico en la siguiente ilustración une las rutas tomadas entre los orígenes y los destinos.

	Destino 1	
	Vínculo	**Mbps**
Origen 1: contabilidad	Frame Relay	0.056
Origen 2: centro de llamadas	Point-to-Point	1.54

	Destino 2	
	Vínculo	**Mbps**
Origen 1: contabilidad	Frame Relay	0.256
Origen 2: centro de llamadas	Frame Relay	1.54

	Destino 3	
	Vínculo	**Mbps**
Origen 1: contabilidad	Frame Relay	0.256
Origen 2: Centro de llamadas	Frame Relay	0.512

Sin embargo, el diseño de interconexiones para adecuarse a las necesidades se parece más a un arte que a una ciencia. Por ejemplo, aún después el total del ancho de banda estimado para un vínculo, debe regresar y dar un colchón para factores como prioridades de QoS, crecimiento disipado a corto plazo, etcétera.

DISEÑOS DE RED DE CISCO

El diseño de redes es una cuestión principalmente de toma de decisiones. Casi todas las decisiones tienen que ver con la selección de las tecnologías y los productos correctos para el trabajo. Aun los elementos de diseño sobre los que no tiene control dependen de dejarle la oportunidad de tomar decisiones. Por ejemplo, si el departamento de arte de la empresa usa AppleTalk y no tiene intención de cambiar, debe decidir si lo ejecuta en vínculos de varios protocolos o lo divide en uno o más segmentos LAN que sólo usan AppleTalk.

Una vez que las necesidades presentes y futuras de la empresa se han investigado y documentado, el siguiente paso consiste en elegir las tecnologías para las diversas áreas funcionales:

- ▼ **Selección de la tecnología de espina dorsal** Existen diversas tecnologías LAN de espina dorsal, y se eligen principalmente con base en el tamaño de la interconexión y en las características de su tráfico.
- ■ **Selección de protocolo** Aquí se supone que IP es el protocolo de red, pero aún debe elegirse cuáles otros protocolos de enrutamiento y control de red habrán de usarse.
- ▲ **Selección de la tecnología de acceso** Una mezcla de concentradores y conmutadores se deben configurar para adecuarse mejor a las necesidades de un grupo de trabajo o aun de un host particular.

Después de que las tecnologías se han erigido, deben configurarse los productos específicos para ejecutarlas. Después de ese paso, debe hacerse más trabajo de diseño para implementar la configuración. Por ejemplo, debe configurarse un modelo de direccionamiento IP, al igual que un subsistema de nombres de servicios, deben afinarse las mediciones de enrutamiento, deben establecerse los parámetros de seguridad, etcétera.

El diseño de interconexiones tiene lugar a dos niveles: el campus y la empresa. Los diseños del campus cubren la red local principal de la empresa, desde el escritorio hacia la espina dorsal de alta velocidad hasta el exterior. El nivel de la empresa abarca varias redes de campus y se concentra en configuraciones WAN (sea una WAN privada de línea arrendada o un sistema basado en Internet entunelado a través de éste).

Diseño lógico de la red

Un diseño de interconexión está definido por una configuración física y una lógica. La parte física se relaciona con el diseño de la topología, los dispositivos de hardware, el software de red, los medios de transmisión y otras piezas. La configuración lógica debe parecerse en gran medida al diseño físico en tres áreas:

- ▼ **Direccionamiento IP** Plan para asignar direcciones de manera racional que puedan conservar espacio de dirección y ajustarse al crecimiento.
- ■ **Servicios de nombre** Plan para permitir que hosts y dominios se direccionen mediante nombres simbólicos en lugar de direcciones IP con puntos.
- ▲ **Selección de protocolos** La decisión de cuáles protocolos usan, sobre todo los protocolos de enrutamiento.

El diseño de interconexiones siempre debe empezar con la capa de acceso, porque las necesidades de mayor nivel no pueden atenderse hasta que el dispositivo y la población de usuarios se conozcan. Por ejemplo, es casi imposible estimar la capacidad hasta que todos los hosts, las aplicaciones y los segmentos LAN se han identificado y cuantificado, y casi todos estos elementos residen en la capa de acceso.

Desde un punto de vista práctico, los tres elementos de diseño lógicos de direccionamiento, asignación de nombres y enrutamiento son buenos como primer paso para empezar a discernir cómo debe disponerse el hardware físico. Cada uno de los tres requiere diseño anticipado y planeación.

Estrategias de direccionamiento IP

El número de direcciones disponibles es denominado *espacio de direcciones*. Las empresas usan varios esquemas de direccionamiento para maximizar el espacio de direcciones dentro de un bloque de direcciones IP que su ISP les ha asignado. Se han ideado varias estrategias de direccionamiento, no sólo para maximizar el espacio de direcciones, sino también para mejorar la seguridad y la capacidad de administración.

Bloques de direcciones IP privadas Una empresa recibe sus direcciones IP públicas de la Internet Assigned Numbers Authority (IANA). Por lo general, ésta sólo asigna direcciones públicas a ISP y empresas grandes, y lo hace como un rango de números, no como una sola dirección IP. En la práctica real, casi todas las empresas reciben sus direcciones IP públicas de su ISP. Cuando se diseñó IP, la IETF reservó tres rangos de direcciones IP para uso como direcciones privadas:

- ▼ De 10.0.0.0 a 10.255.255.255
- ■ De 172.16.0.0 a 172.31.255.255
- ▲ De 192.168.0.0 a 192.168.255.255

Estos tres bloques de direcciones IP se reservaron para editar confusiones. Usted puede usar direcciones dentro de cualquiera de estos bloques reservados sin miedo de que uno de sus enrutadores empiece a confundirse con no se encuentra la misma dirección en el exterior, porque son direcciones privadas que nunca parecen en Internet.

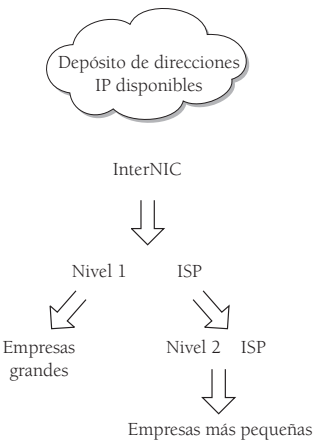
Las direcciones IP privadas son asignadas por un equipo de red a los dispositivos internos. Debido a que nunca se usan fuera de los sistemas autónomos, las direcciones privadas pueden asignarse siempre y cuando permanezcan dentro del rango asignado. No se necesita una autorización de la IETF ni de cualquier otro cuerpo de coordinación para usar las direcciones privadas, que se usan por estas razones:

- ▼ **Conservación del espacio de direcciones** A pocas empresas se les asignó un número suficiente de direcciones IP públicas para incluir todos los nodos (hosts y dispositivos) dentro de su interconexión.
- ■ **Seguridad** Las direcciones privadas se traducen mediante PAT o NAT al exterior. Al desconocerse la dirección privada es más difícil para los hackers irrumpir en un sistema autónomo pretendiendo ser un nodo interno.
- ■ **Flexibilidad** Una empresa puede cambiar ISP sin tener que cambiar ninguna de sus direcciones privadas. Por lo general, sólo necesitan cambiarse las direcciones de los enrutadores o firewalls que realizan traducción de direcciones.

- **Tablas de enrutamiento más pequeñas** Al hacer que muchas empresas anuncien sólo uno y en otro unas cuantas direcciones ayuda a minimizar el tamaño de la tabla de enrutamiento en uso de enrutadores de Internet, con lo que mejora el desempeño.

Este último elemento tal vez explique por qué la IETF estableció una dirección IP de 32 bits en lugar de un diseño de 64 bits. El uso de un espacio de direcciones infinitamente grande hubiera desanimado el uso de las direcciones privadas. El uso de las direcciones IP globales sería indiscriminado, haciendo enormes las tablas de enrutamiento del proceso. Esto crearía la necesidad de que los enrutadores tuvieron CPU más rápidos y grandes cantidades de memoria. De regreso al momento en que se diseñó IP durante la década de 1970, los dispositivos de red estaban en su infancia y eran muy lentos y tenían una configuración deficiente de acuerdo con los estándares de hoy en día.

Obtención de direcciones IP públicas Las direcciones IP registradas deben comprarse a la AINA, que es una organización no lucrativa y responsable de asegurar que dos empresas no tengan asignadas direcciones IP duplicadas. Pero pocas empresas obtienen sus direcciones IP directamente de la IANA; la mayor parte de ellas lo tienen indirectamente a través de su ISP.



Por ejemplo, los ISP de capa 1, como LUNET o Sprint, aseguran grandes bloques de direcciones IP de la IANA. Ellos a su vez los pasan a ISP de capa 2 (probablemente haya docenas de ellos tan sólo en su ciudad), que, a su vez, los asignan a empresas de usuario final. Casi todas las compañías grandes tratan directamente con ISP de nivel 1. Las direcciones IP se entregan en bloques. Cuanto mayor sea su empresa, mayor será el rango de direcciones IP que debe obtener.

Direccionamiento dinámico El direccionamiento dinámico es una técnica mediante la cual se asignan direcciones IP a los hosts del sistema final en el momento del inicio de sesión. Novell NetWare y AppleTalk han tenido capacidades de direccionamiento dinámico integrados desde el principio. Sin embargo, ése no es el caso con IP. Recuerde que los protocolos de escritorio como NetWare IPX fueron diseñados con el modelo cliente-servido en mente, mientras que IP se diseñó originalmente para conectar un sistema mundial: el reaccionamiento dinámico IP de Internet sólo saltó al primer plano a mediados de la década de

1980 para acomodar las estaciones de trabajo sin disco que no tenían en dónde almacenar direcciones IP permanentes.

Un par de protocolos iniciales de asignación de dirección IP dinámico del desarrollo del Host Dynamic Configuration Protocol (DHCP, protocolo dinámico de configuración de host). DHCP ahora es el estándar *de facto*, usa un modelo cliente-servidor en que un servidor mantiene una lista actualizada de direcciones disponibles y la asigna a medida que se soliciten. DHCP también puede usarse como herramientas de configuración. Soporta asignación permanente automática de direcciones IP a un nuevo host y se usa incluso para asignaciones manuales de direcciones como una manera de comunicar la nueva dirección al host cliente. En la figura 14-7 se describe el proceso de DHCP.

La asignación dinámica es popular porque resulta fácil de configurar y conserva el espacio de direcciones. DHCP funciona al asignar direcciones por un periodo llamado *arrendamiento*, lo que garantiza que no se asigna la dirección IP a otro host, siempre y cuando esté arrendado. Cuando el host terminó la sesión en la red, el servidor DHCP recibió la notificación y restaura la dirección a su almacén de direcciones disponibles.

Para asegurar el servicio, a menudo se configuran varios servidores DHCP. Cuando el host inicia sesión, envía un mensaje de descubrimiento de DHCP en la red al servidor espe-

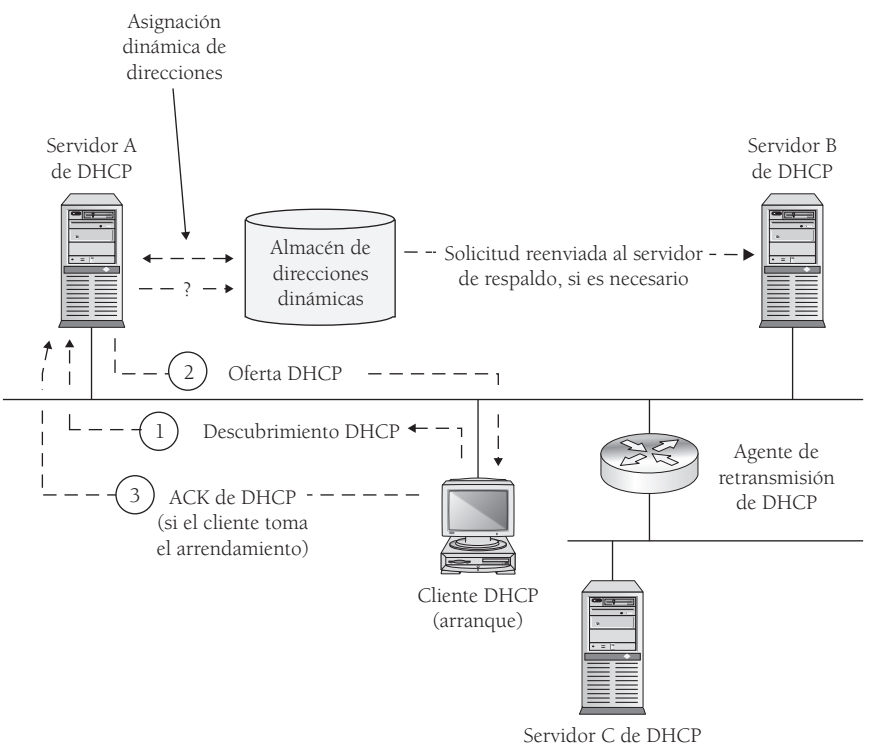


Figura 14-7. DHCP puede asignar direcciones IP dinámicamente a hosts de extremo de sistemas.

cificado mediante el campo identificador del mensaje DHCP. El servidor DHCP responde con un mensaje de oferta de DHCP o pasa la solicitud de descubrimiento a un servidor de respaldo. El cliente acepta la oferta al enviar al servidor un mensaje ACK de DHCP como reconocimiento.

Si se acepta la oferta, el servidor bloquea el arrendamiento en el almacén de direcciones disponibles al mantener la asignación en memoria persistente hasta que se termine el arrendamiento. La terminación de éste ocurre cuando el cliente sale de la red (lo que se completa por lo general cuando el usuario apaga su PC al final del día). Si el servidor DHCP identificado deja de funcionar o rechaza la solicitud, después de un periodo de espera preestablecido, el cliente puede configurarse para enviar una solicitud de descubrimiento a un servidor DHCP de respaldo. Si el servidor no se encuentra en la misma subred, puede configurarse un enrutador como un agente de retransmisión de DHCP para dirigir el mensaje de solicitud al segmento LAN en que reside el servidor.

Sistema de nombres de dominio

Como se analizó en esa revisión de los fundamentos de las interconexiones en el capítulo 2, las personas casi siempre llegan a los nodos de cliente por nombre, no por dirección. Piense en esto: ¿cuántas veces ha escrito una dirección IP con puntos en el campo de direcciones de su explorador? En casi todos los casos, escribe un URL en lugar de eso, o simplemente hace clic en uno que se encuentra detrás de un vínculo de hipertexto en una página Web.

El servicio usado para asignar nombres en Internet se denomina Domain Name System (DNS, sistema de nombres de dominio). Un nombre DNS tiene dos partes: el nombre del host y el nombre del dominio. Tome como ejemplo toby.velte.com, toby es el host (en este caso, la PC de una persona) y velte.com es el dominio. Hasta el 2000, los nombres de dominio tenían que registrarse con InterNIC (Internet Network Information Center), una agencia del gobierno de Estados Unidos. Sin embargo, esa responsabilidad se transfirió a varias empresas privadas, sacando al gobierno del negocio de los URL.

La IETF ha especificado que los sufijos de nombre de dominio sean asignados con base en el tipo de organización que es el sistema autónomo, como se presenta en la lista de la tabla 14-2.

También hay dominios de alto nivel geográfico definidos por país; por ejemplo, .fr para Francia, .ca para Canadá, .de para Alemania (como en Deutschland), etcétera. Para que los dominios funcionen, deben, en algún punto, correlaciónase con una dirección IP para que

Dominio	Tipo de sistema autónomo
.com	Compañía comercial
.edu	Institución educativa
.gov	Agencia gubernamental
.org	Organización no lucrativa
.biz	Restringida a los negocios

Tabla 14-2. Sufijos de nombre de dominio IETF.

los enrutadores puedan reconocerlos. A esta correlación se les denomina *resolución de nombres* (una tarea realizada por los servidores de nombres). Los sistemas de nombres de dominio distribuyen bases de datos entre muchos servidores para satisfacer las solicitudes de resolución. Una empresa grande distribuía su base de datos DNS a través de su topología de interconexión. La gente puede hacer clic y recorrer Internet debido a que sus bases de datos DNS están distribuidas en todo el mundo. En la figura 14-8 se describe el proceso de servicios de nombres.

Cuando un cliente necesita enviar un paquete, debe correlacionar el nombre simbólico del destino con su dirección IP. El cliente debe tener lo que se denomina software de resolución configurado para hacer esto. El software de resolución del cliente envía una consulta a un servidor DNS local, recibe la resolución, escribe la dirección IP en el encabezado del paquete y lo transmite. La asignación de nombre a IP se mantiene en el caché del cliente por un periodo preestablecido. Mientras el cliente tenga la asignación para un nombre en caché, omite el proceso de consulta por completo.

Configuración del servidor de nombres Muchas interconexiones tienen varios servidores DNS para proporcionar más velocidad y redundancia, sobre todo en sistemas autónomos más grandes en que los hosts frecuentemente van y vienen. Por lo general, los servicios de nombres se mantienen a partir del servidor central dentro de la interconexión. Por ejemplo, las redes de Windows 2000/2003 tienen los llamados servidores de Domain Control (DC, control de dominio), que es responsable de varias tareas de limpieza, incluidas las solicitudes de inicio de sesión.

Además de DNS, los otros dos principales servicios de asignación de nombres son el Windows Internet Name Service (WINS), y Network Information Service (NIS) de Sun Microsystems. Mientras que DNS está optimizado para asignaciones de Internet, WINS y NIS manejan servicios de nombres en el nivel de las interconexiones. Los servidores WINS usan DHCP para solicitudes de campo, porque DNS no se presta al manejo de nombre dinámico. (Los quiere almacenados permanentemente.) NIS realiza una tarea similar entre hosts de UNIX.

DNS es un estándar importante. Puede hacer clic entre los hosts de todo el mundo porque hay cientos de miles de servidores DNS en todo el globo, intercambiando e incluyendo en caché las asignaciones de nombres entre dominios de agrupamientos para que a éste le tome un mínimo de tiempo conectarse a un nuevo sitio Web.

Diseños de red de campus

El término *red de campus* es un poco confuso. Lo que significa que es cualquier interconexión local con una espina dorsal de alta velocidad. Por ejemplo, la red local de las oficinas centrales de una empresa localizada por completo en un rascacielos es un ejemplo de una red de campus. El término ha llegado a usarse de manera tan amplia en el mercado de la computación, que es asestado como el término para las redes locales de tamaño medio y grande. Sin importar cómo se le llame, se despliegan varios modelos para configurar redes de campus. Los revisaremos aquí.

La configuración conmutador-enrutador

La llamada configuración conmutador-enrutador cubre el acceso y la distribución de capas del modelo de diseño de red jerárquico de tres capas. Las dos capas están consideradas jun-

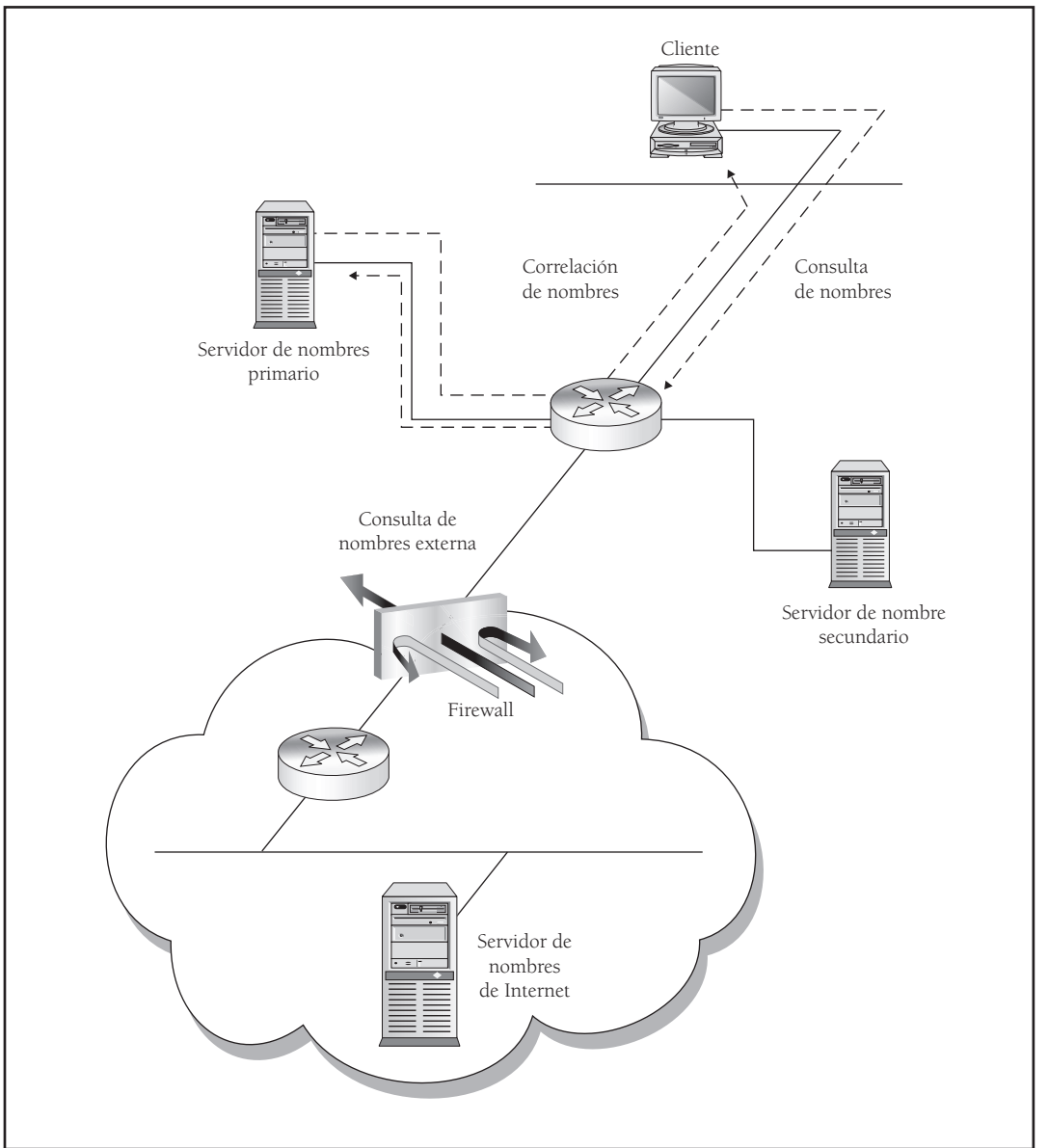


Figura 14-8. Los nombres de dominio deben resolverse en un servidor de nombres.

tas debido a que los enrutadores de distribución suelen localizarse en el mismo edificio que los dispositivos hosts que dan acceso a la red.

Configuración de capas de acceso La capa de acceso del modelo jerárquico de tres capas es en gran medida una función de la denominada configuración conmutador-enru-

tador. La principal excepción a esto es el acceso remoto, que se cubre más adelante en este capítulo (consulte la sección titulada "corrección a sitios remotos"). La configuración de la capa de acceso se relacionó principalmente con la conexión de los costos en un departamento o un piso de un edificio. En cuanto a los medios físicos, supondremos que se usa cable Unshielded Twisted Pair (UTP, par trenzado sin protección) para conectar a los hosts en los dispositivos de acceso.

Una consideración importante que debe tomarse en cuenta cuando se configuran las capas de acceso y distribución, es qué tipo de red se estará desplegando. Casi todos los secretos LAN de la capa de acceso que se diseñan hoy en día se ejecutan en la especificación Fast Ethernet, la variante de 100 Mbps del estándar Ethernet.

Estas decisiones determinan lo que los productos de Cisco configuran y, en cierta medida, cómo se distribuye su topología.

Selección de la tecnología de capas de acceso Hoy en día, si tiene una opción, es mucho mejor que use Fast Ethernet para la capa de acceso. Es rápida, económica y el grupo de talento de los administradores de red conoce mejor estas especificaciones LAN. Por ejemplo, si tiene 10 Mbps Ethernet, sus opciones están un poco más limitadas. También debe tener el cuidado de que cualquier cable existente satisfaga los requisitos físicos especificados por la tecnología LAN.

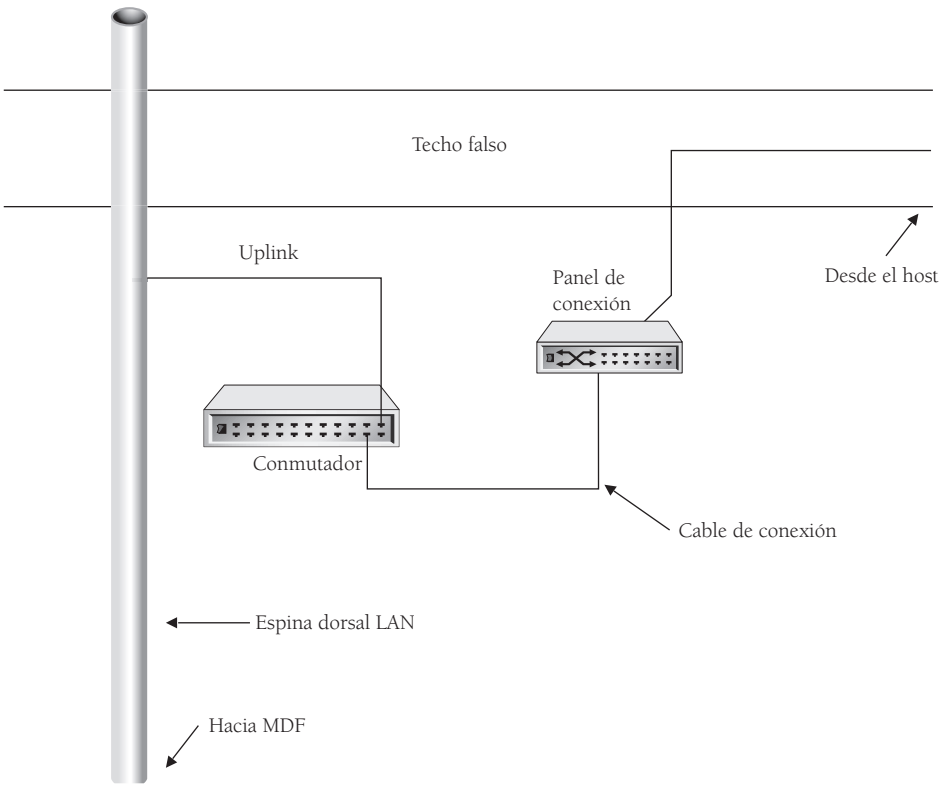
Es un poco más complicado conocer la manera inexacta en que habrá de distribuir la capa de acceso. Se ha reunido la información de análisis de necesidades que se trató antes, esos datos habrán de indicarle dos cosas importantes:

- ▼ **Jerarquía del grupo de trabajo** Los grupos de trabajo homogéneos grandes tienden a prestarse a las redes conmutadas planas. Por ejemplo, los departamentos grandes de servicio a clientes o de ayuda de escritorio tienden a conectar un conjunto muy consistente de hosts para ejecutar un conjunto limitado de aplicaciones. Estas distribuciones son estupendas candidatas para redes conmutadas planas (no VLAN).
- ▲ **Cargas de tráfico** Si los volúmenes de tráfico serán pesados y las directivas de QoS serán rígidas, tal vez quiera analizar una red conmutada VLAN o por lo menos una configuración de red enrutada de ancho de banda elevado.

Mientras responde estas dos preguntas para varias áreas de su topología, la configuración empieza a tomar forma. Con mucha frecuencia, ese proceso se repite piso por piso y edificio por edificio. Esto no debe sorprenderle. Después de todo, el trabajo en red no es el único campo de acción que tiene una naturaleza geográfica. Es igual que la administración de operaciones; por lo general tiene sentido que los administradores agrupen ciertos tipos de trabajadores o ciertos tipos de tareas de trabajo dentro de un lugar físico.

Disposición física La topología clásica de la capa de acceso es el diseño del MDF en el clóset. Un clóset de datos (también denominado **clóset alambrado** o **clóset de teléfonos**) es un pequeño cuarto que incluye paneles de conexión que conectan a hosts y concentradores o puertos conmutados de acceso. El panel de conexión es el lugar en el que inician a las redes. Un panel de conexión es un dispositivo pasivo con filas de conectores RJ-45 similares a los conectores RJ-11 de los teléfonos. El cable de par trenzado sin protección del dispositivo se conecta en un conector, y un cable de otro conector se conecta en el puerto del conmu-

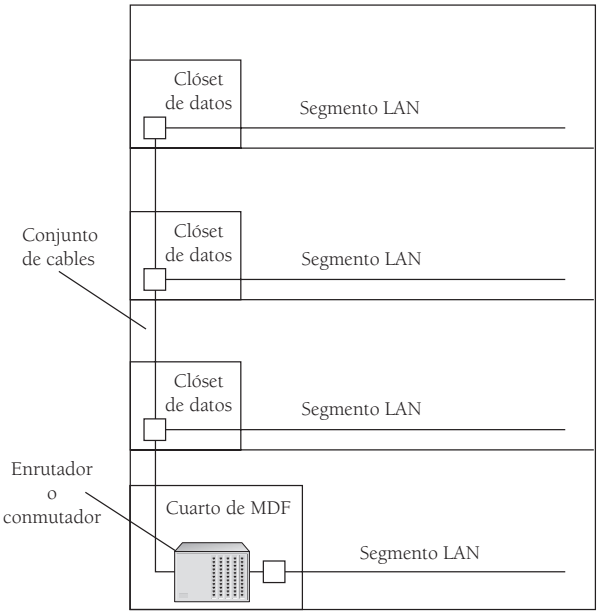
tador. Esta organización modular le da gran flexibilidad al desplazamiento de dispositivos entre puertos.



Las señales atraviesan el conmutador al salir de su puerto uplink para conectarse al grupo de cables individuales que recorren los pisos hacia el punto de terminación del edificio. Un uplink conecta el conmutador "hacia arriba" en el sentido lógico, porque el conjunto de cables se dirige hacia una pieza grande del equipo (por lo general, un enrutador o un conmutador LAN).

MDF son las siglas de *Main Distribution Facility* (*instalación principal de distribución*), que es por lo general un cuarto en una ubicación segura del primer piso del edificio. La MDF sirve como el fondo de terminación para el cableado que emana de los clósets de datos, que a menudo es equipo para voz y datos. La tendencia ha sido localizar el MDF en el cuarto de cómputo de la empresa, si hay uno en el edificio. Dependiendo de la configuración del edificio, la espina dorsal viaja a través de los agujeros hechos a través de los pisos o por el cubo del elevador.

En edificios más grandes, el medio de transporte es casi siempre cable de fibra óptica. La razón principal para usar este cable es que puede transportar los datos más de 100 metros y no se ve afectado por el ruido eléctrico en los edificios.



La configuración del conmutador Se aplican varias reglas cuando se configura la capa de acceso. El cable UTP puede abarcar hasta 100 m desde el clóset de datos. Esto casi siempre es más que suficiente en un plano horizontal. (Pocas áreas de trabajo son más anchas que un campo de fútbol.) Si el clóset de datos se localiza en el centro de un piso, el ancho efectivo sería de 200 m. Como se muestra en la figura 14-9, no todos los edificios son verticales. Muchas son estructuras horizontales largas de uno o dos pisos, como las plantas de producción y los almacenes. El caso de esos pisos muy largos, la práctica es colocar los clóset de datos en ambos lados.

Desde un punto de vista lógico, no tiene sentido colocar a un enrutador en cada piso. Hacerlo así sería prohibitivamente caro. Entonces, la estrategia consiste en minimizar el número de interfaces de enrutador que dan servicio a un número determinado de hosts. Los conmutadores realizan esto. En la figura 14-9 se muestra una configuración para una compañía de tamaño medio que tiene unos cuantos cientos de empleados en un edificio. Para conectar los usuarios de cada piso, por lo menos se coloca un Cisco Catalyst 3750 en cada clóset de datos. Este modelo conecta a 12, 24 o 48 hosts por unidad y permite apilar hasta nueve unidades por pila. El tamaño de la pila depende del número de empleados en el piso. El modelo particular de Catalyst 3750 que usen dependerá de la densidad de la población: algunos modelos soportan 12 puertos por una densidad de pila de 108 puertos y otro soportan 48 puertos para una densidad de 432 puertos. Si la población supera los 432, simplemente ponga otra pila en el clóset de datos para aumentar el número de puertos.

En el área de la parte inferior izquierda de la figura 14-9 se muestra un conjunto de cables que no es la espina dorsal en el sentido apropiado del término. El uplink que sale del Catalyst 3750 en la planta baja expande el conjunto de cables a un total de cinco cables de fibra óptica, que son cables esencialmente largos usados para evitar la colocación de dispositivos terminales en cada piso. La espina dorsal se define lógicamente, de modo que puede considerar al conjunto de cables como “cables de alimentación” en lugar de espina dorsal.

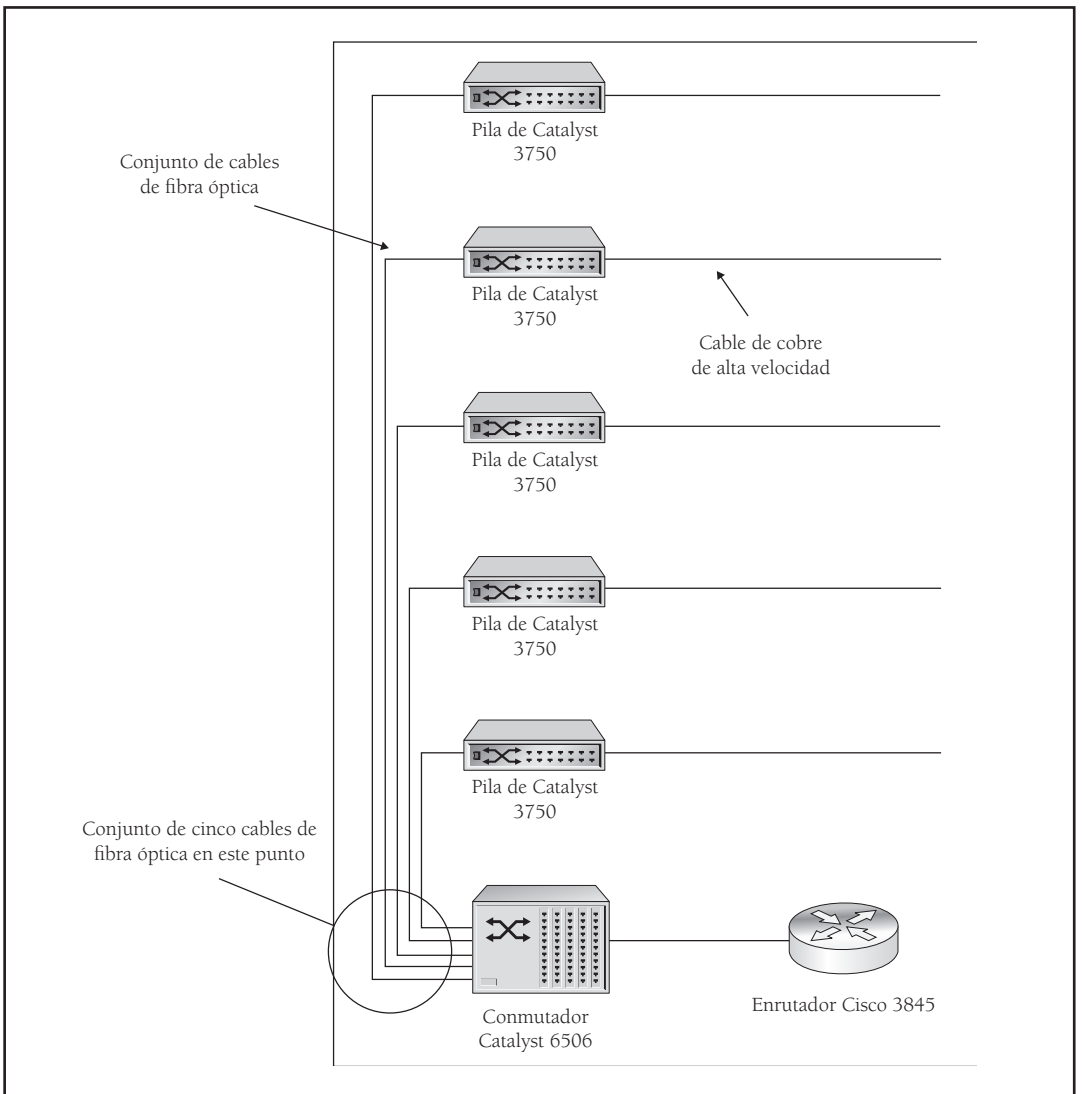


Figura 14-9. La configuración clásica enrutador-conmutador emplea conmutadores más pequeños conectados a un conmutador más grande, que luego se conecta a un enrutador.

La tecnología LAN utilizada en todo este edificio de ejemplo es Fast Ethernet, que transporta 100 Mbps. Esa velocidad es suficiente para conectar casi todos los dispositivos hosts individuales. En términos prácticos, esto significa que nuestro conjunto de cables se dirige a la MDF con un ancho de banda neto de 500 Mbps, de modo que se necesita un dispositivo rápido para manejar las conexiones. Hemos configurado un conmutador Cisco Catalyst 6506 para el trabajo. Con un plano posterior de 32 Gbps, el Catalyst 6506 tiene la suficiente potencia para mantener una velocidad de transmisión de datos satisfactoria para el tráfico de los cinco

segmentos LAN. Esta caja tiene seis ranuras de módulo, pero una sola tarjeta 100FX de 12 puertos puede manejar a los cinco segmentos LAN, dejando mucho espacio para el crecimiento. Una segunda ranura se usa para conectar al exterior, dejando tres ranuras abiertas.

En la figura 14-9 se dibuja la ventaja inherente de la conmutación LAN. Recordarán del capítulo 5 que un conmutador es casi 10 veces más rápido cuando tiene direcciones MAC en su tabla de conmutación. Nuestra compañía de ejemplo tiene 300 empleados, y el Catalyst 6506 tiene una memoria más que adecuada y una velocidad en el plano posterior para manejar una tabla de conmutación de ese tamaño. (Puede manejar miles.) Debido a que el conmutador está hablando con más de 300 hosts, tiene sus direcciones MAC disponibles.

Configuración del conmutador de acceso Ya hemos mencionado que los concentradores han dado paso a los conmutadores. De lo que hablamos aquí es de la *conmutación de acceso*, en oposición al ejemplo de conmutación LAN de la figura 14-9. Un conmutador conecta los hosts a un segmento LAN. Esto extiende el ancho de banda conmutado hacia el escritorio o el servidor. En la figura 14-10 se muestra una configuración de conmutador de acceso típico.

No sería práctico utilizar un cable de fibra óptica hasta la MDF para cada host conmutado. Como se muestra en la figura 14-10, un paso intermedio puede ser configurar el uso de un conmutador de acceso como Cisco Catalyst 2820, capaz de conectar hasta 24 dispositivos. Un conmutador del extremo inferior no se usa aquí porque no tiene un puerto FX para conectar a un conjunto de cables de fibra óptica.

Debe destacarse que en los entornos de alta densidad, los usuarios se enfrentan a la configuración de conmutadores Catalyst del extremo alto en el clóset de datos o la conexión de cables a la MDF.

La configuración de un conmutador y un enrutador Para que tengan la capacidad de interconectarse, los usuarios necesitan enrutarse en algún punto. La práctica estándar consiste en configurar un enrutador local en el cuarto de MDF. De esa manera, los usuarios dentro de la empresa están conectados a la interconexión empresarial para comunicaciones intramuros, además del firewall para conectarse a Internet.

En la figura 14-11 se hace un acercamiento al cuarto MDF de nuestra empresa de ejemplo. Un enrutador Cisco 3845 está configurado en esta situación porque tiene ocho ranuras de módulo que pueden acomodar módulos LAN o WAN. Una ranura está ocupada con un módulo LAN 100BaseTX de un puerto para conectar el conmutador Catalyst 6500; el otro alberga un módulo T1 WAN de un puerto que conecta al edificio con el mundo exterior.

Si está pensando que con todo el ancho de banda que se encuentre en ese edificio, tal vez no sea suficiente una simple conexión de 1.544 Mbps al exterior, se está dando cuenta de que un vínculo T1 en realidad puede no ser suficiente, dependiendo de la cantidad de la carga del tráfico local que fluye hacia el exterior.

La nueva regla 80/20 ¿Recuerda la regla 80/20 analizada en páginas anteriores de este capítulo (consulté la sección "El modelo de diseño jerárquico de tres capas")? La tradición dictó que sólo 20% del tráfico vaya el exterior. Pero las cosas han cambiado. Ahora los gurús están hablando acerca de la "nueva regla 80/20", también conocida como la regla 20/80, donde hasta el 80% del tráfico puede ir al exterior mientras los usuarios utilizan Internet para descargar archivos, hablar con otras partes de la intranet de la empresa o incluso tratar con socios comerciales a través de una extranet.

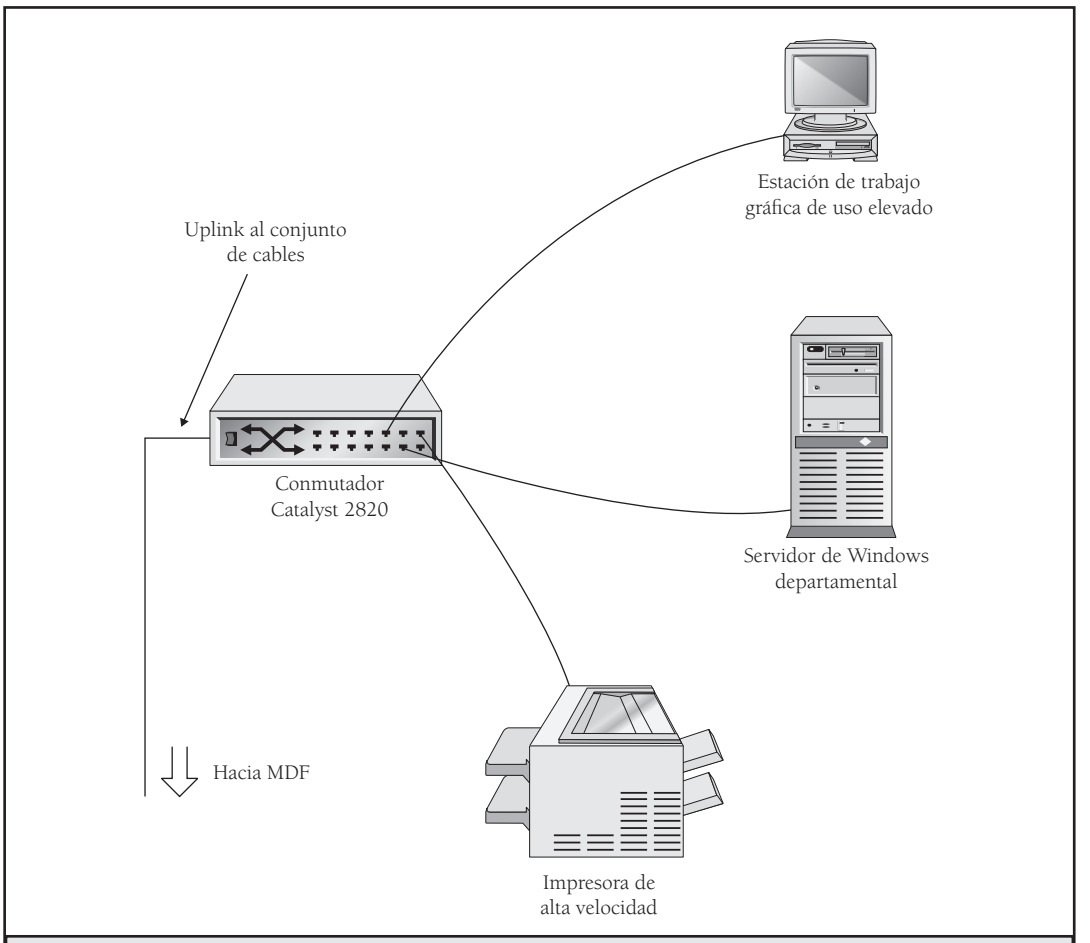


Figura 14-10. Los conmutadores de acceso reemplazan a los puertos concentradores para conectar a los hosts hambrientos de ancho de banda.

El mayor impulsor que está dando vuelta a la regla 80/20 es el comercio electrónico, de donde las computadoras de la red están hablando en transacciones de ventas tradicionalmente realizadas por los seres humanos. Los sitios Web como Amazon.com y E*TRADE son famosos por cortar los intermediarios humanos, pero el comercio electrónico de negocio a negocio, llamado Electronic Data Interchange (EDI, intercambio electrónico de datos), está generando más tráfico IP tras cada día que pasa.

Suponiendo que la nueva regla 80/20 se mantiene para nuestra empresa de ejemplo, el cuarto MDF podría configurarse de acuerdo con las líneas establecidas en la figura 14-12, donde una conexión mucho más amplia se extiende al exterior en la forma de una línea T3 (un medio de vínculo WAN digital, de línea arrendada, a 43 Mbps).

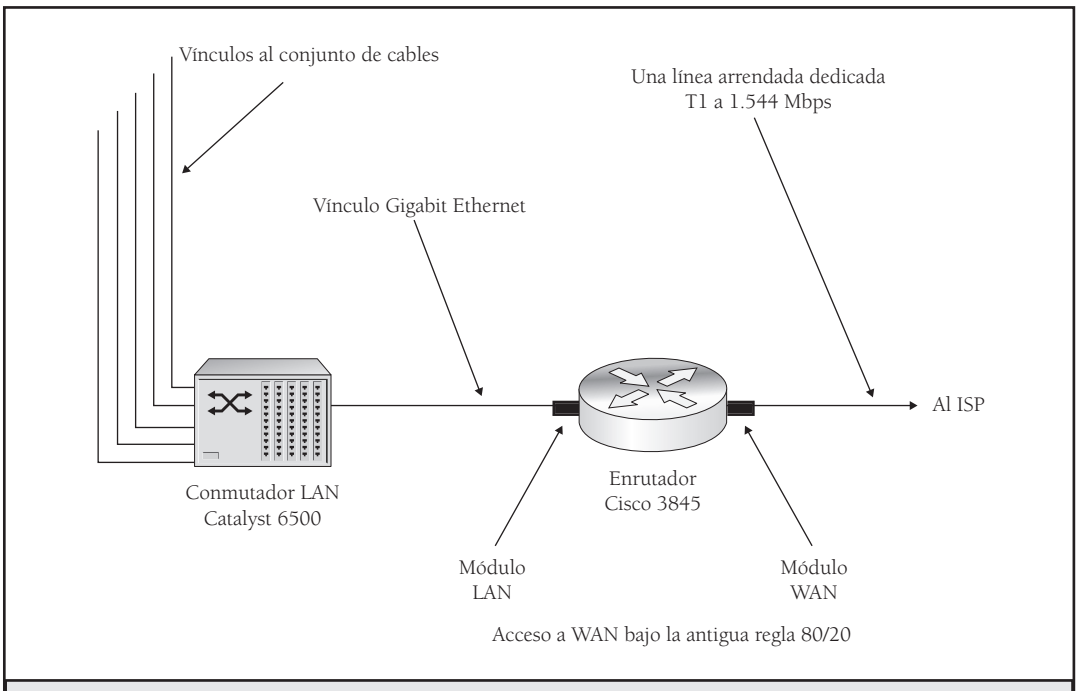


Figura 14-11. Las redes conmutadas necesitan que los enrutadores hablen con el mundo exterior.

Ahora el enrutador es más grande y el conmutador es más pequeño. Si los usuarios están hablando al exterior 80% del tiempo, es menor la necesidad de conmutar el tráfico dentro del edificio. Hemos configurado un conmutador Cisco Catalyst 2900 en lugar del Catalyst 6500 porque hay que hacer menos trabajo de conmutación LAN. El enrutador Cisco 7206 está configurado para una mayor capacidad de transmisión de datos, con un procesador más rápido y un chasis de seis ranuras.

A 45 Mbps, T3 se ejecuta casi 30 veces más rápido que una línea T1. Cada vez más empresas están usando T3 para hacer las conexiones de punto a punto con su ISP. Sin embargo, pocos necesitan toda la capacidad, de modo que casi todos los ISP revenden una parte del ancho de banda a clientes individuales de acuerdo con sus necesidades, una práctica a la que se le llama *fraccionamiento*, en que el cliente se inscribe por sólo una fracción de la capacidad del vínculo.

Elección de una espina dorsal de alta velocidad

Las espinas dorsales se usan para conectar nodos importantes de red de igual a igual. Un vínculo de espina dorsal conecta dos nodos particulares, pero el término *espina dorsal* a menudo se hace para aludir a una serie de vínculos de espina dorsal. Por ejemplo una espina dorsal de campus podría extenderse sobre varios vínculos.

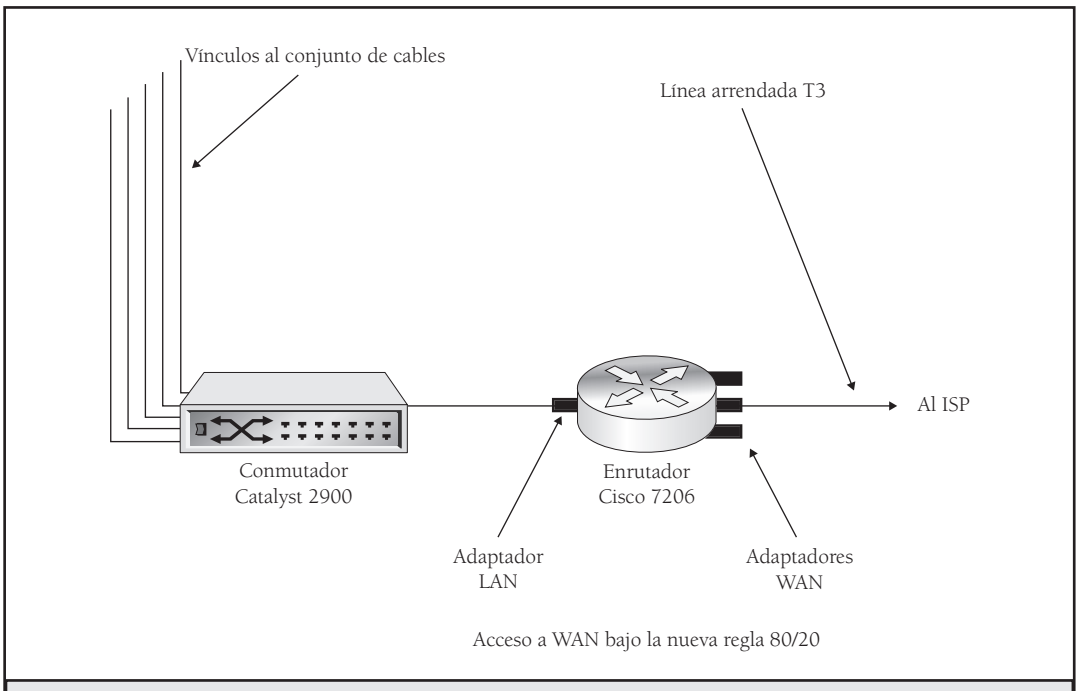
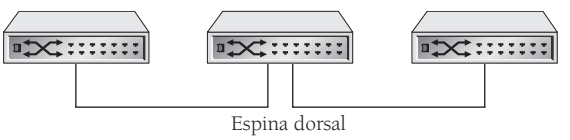


Figura 14-12. El uso pesado de Internet está llevando a las empresas a instalar enrutadores más grandes de orilla.



Los vínculos de espina dorsal mueven los datos entre dispositivos de espina dorsal únicamente. No manejan tráfico entre los segmentos LAN dentro de un sitio. Eso se hace en la capa de distribución de este modelo jerárquico de tres capas a través de conmutadores y enrutadores LAN. Las espinas dorsales se concentran en nombre del tráfico a velocidades muy elevadas en tierra.

Las espinas dorsales de campus obviamente recorren una corta distancia, por lo general a través de cableado de fibra óptica subterránea. Las espinas dorsales WAN (usadas por empresas e ISP) mueven el tráfico entre ciudades. Casi todos los vínculos de espinas dorsales WAN son operados por los denominados proveedores de espina dorsal de Internet, aunque muchas empresas grandes operan sus propios vínculos de larga distancia de alta velocidad. Los vínculos WAN corren sobre vínculos de cable de fibra óptica de alta velocidad tendido bajo tierra, en postes de electricidad y hasta debajo de los océanos. Los vínculos de satélite también se están volviendo comunes. Sin importar el medio de transporte y si se trata de una espina dorsal de campus o WAN, comparten las siguientes características:

- ▼ **Manipulación mínima de paquetes** El procesamiento de elementos como la imposición de lista de control de acceso y el filtro de firewall se mantiene fuera de la espina dorsal para agilizar la velocidad de transmisión de datos. Por esta razón, casi todos los vínculos de espina dorsal son conmutados, no enrutados.
- ■ **Dispositivos de alta velocidad** Un dispositivo relativamente lento como el Cisco 4500 no se configuraría en una espina dorsal de alta velocidad. Los dos extremos de un vínculo de espina dorsal por lo general operan sobre vínculos de Catalyst 6500 o más rápidos.
- ▲ **Transporte rápido** Casi todas las espinas dorsales de alta velocidad están construidas sobre tecnología de transporte de 1 Gbps o mayor.

Las dos principales tecnologías de espina dorsal son ahora ATM y Gigabyte Ethernet. FDDI está instalado ampliamente, pero con una capacidad total de sólo 100 Mbps, pocas nuevas instalaciones de FDDI están conectándose a espinas dorsales de alta velocidad.

Espinas dorsales ATM Asynchronous Transfer Mode (ATM, modo de transferencia asincrónico) usa un formato de longitud física en lugar de los paquetes de longitud variable que usa Ethernet. El formato de longitud física se presta a una transmisión de datos de alta velocidad, porque el hardware siempre sabe exactamente dónde empieza cada celda. Por esta razón, ATM tiene una relación positiva entre carga útil y tráfico excedente de control de red. Esta arquitectura también se presta a QoS (una enorme opción adicional para vínculos de espina dorsal de operación crítica).

En la figura 14-13 se muestra una espina dorsal de campus construida sobre ATM. La configuración usa conmutadores LAN Catalyst 6509 para el edificio externo y un enrutador conmutado Catalyst 8500 Multiservice para manejar el tráfico que llega al conjunto de servidores central de la empresa.

Una *cuchilla* es un término de la industria para una tarjeta de circuito impresa de gran tamaño que es básicamente un dispositivo de red completo en un solo módulo. Las cuchillas se insertan en las ranuras del gabinete. Para que un conmutador Catalyst hable en ATM, la cuchilla adaptadora apropiada debe configurarse en el gabinete. La cuchilla LightStream 1010 se usa aquí porque está diseñada para tráfico de corto alcance (no hay otras cuchillas ATM "de borde" para tráfico WAN. Una razón para esto es permitir que Cisco soporte diferentes tecnologías en un solo producto.

Los dispositivos ATM de Cisco usan la tecnología de adaptador LAN Emulation (LANE, emulación LAN) para integrarse con las redes Ethernet de campus.

Las espinas dorsales WAN conmutadas corren sobre troncales de fibra óptica de muy alta velocidad que ejecutan la especificación SONET. La mayor parte de las nuevas troncales que se están impulsando son OC-48, que corren a casi 2.5 Gbps. OC (son las siglas de Optical Carrier, portadora óptica) y SONET las de Synchronous Optical NETwork (red óptica sincrónica). Se trata de un estándar desarrollado por Bell Communications Research para redes de muy alta velocidad sobre cable de fibra óptica. La especificación SONET más lenta, OC-1, corre a 52 Mbps (casi la misma velocidad que T3). OC SONET es una tecnología importante, porque representa la "tubería" de infraestructura de más alta velocidad que necesita Internet para seguir expandiéndose. Mencionamos esto aquí porque los esfuerzos de investigación y desarrollo de ATM y Gigabyt Ethernet se están realizando con la especificación SONET en mente, y es el transporte de vínculo WAN supuesto.

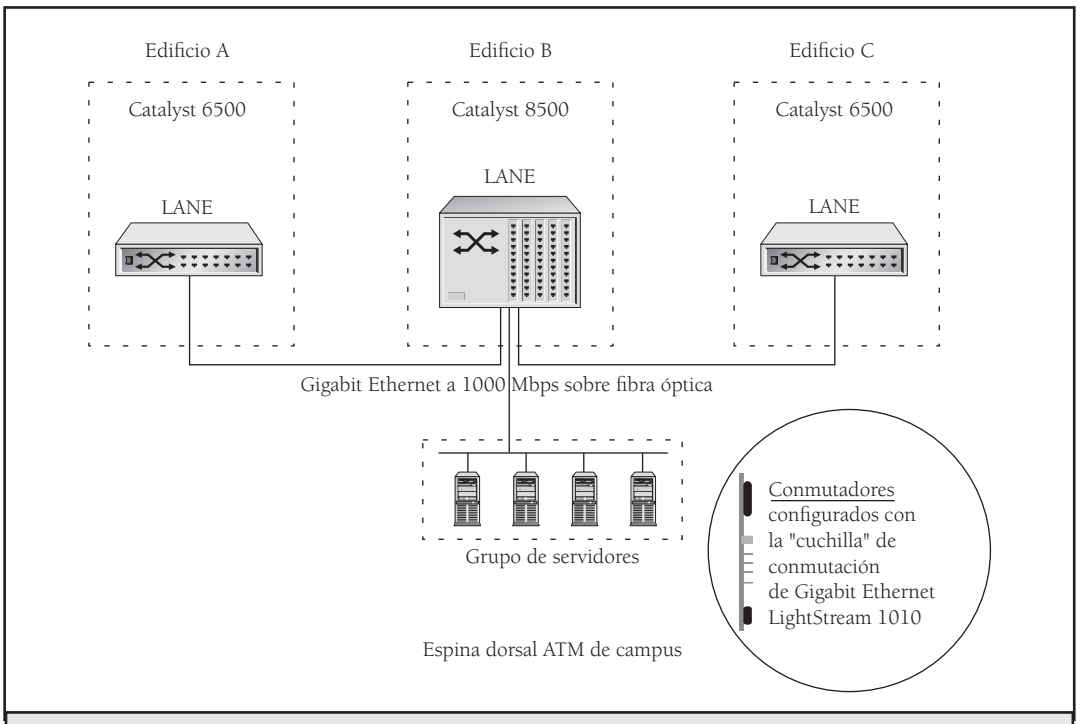


Figura 14-13. Una espina dorsal de campus ATM puede conectar recursos centrales.

Espina dorsal Gigabit Ethernet Aunque Gigabyt Ethernet es una tecnología mucho más reciente que ATM, muchos administradores de redes están cambiándose a ella para satisfacer sus necesidades de espina dorsal en lugar de ATMN. En la figura 14-14 se muestra que la espina dorsal Gigabyt Ehernet puede configurarse usando las mismas plataformas Catalyst que para ATM, esto se hace al configurar cuchillas Gigabyt Ethernet en lugar de cuchillas ATM. Tome en cuenta, también, que el mismo cableado de fibra óptica puede usarse para Gigabyt Ethernet en lugar de ATM.

Como podrá imaginar, las cuchillas y los adaptadores específicos de la tecnología representan las diferentes necesidades electrónicas para procesar paquetes Ethernet de longitud variable o celdas ATM de longitud fija.

Conexión a sitios remotos

Los tipos de ubicaciones remotas: las sucursales y la pequeña oficina u oficina en casa. La diferencia definitiva entre ambas es el tipo de conexión. Debido a que sólo tienen uno o dos usuarios en línea en un momento determinado, las oficinas en casa o pequeñas oficinas usan conexiones de mercado telefónico, mientras que los sitios de sucursales usan alguna forma de circuito dedicado. Tres tecnologías de conexión remota importantes están configuradas aquí. Tal vez quiera regresar al capítulo 2 para revisar la manera en que funcionan esas tecnologías.

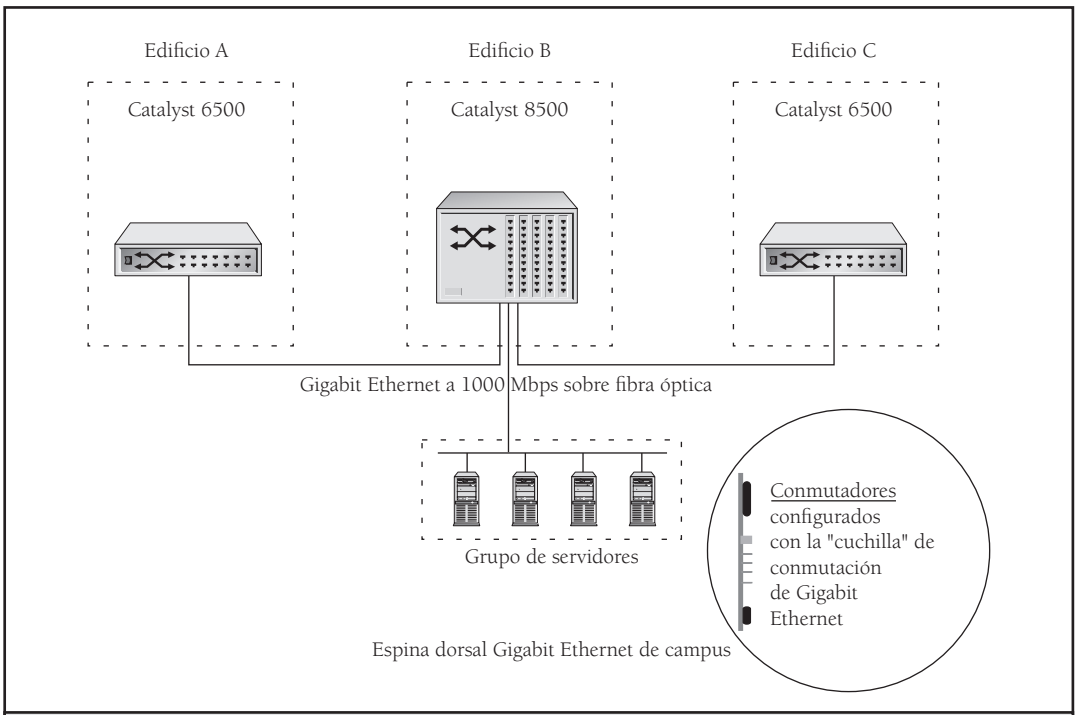


Figura 14-14. Gigabyt Ethernet también puede ejecutarse en conmutadores Catalyst de alto desempeño.

Frame Relay Frame Relay es ideal para tráfico WAN "intermitente". En otras palabras, las líneas arrendadas dedicadas como T1 o T3 sólo tienen sentido económico si se utilizan de manera continua. Frame Relay resuelve ese problema al dejar que los usuarios compartan infraestructura WAN con otras empresas. Frame Relay puede ser esto porque es una Packet-Switched Data Network (PSDN, red de datos de paquetes conmutada), en que las conexiones de extremo a extremo son virtuales. Sólo necesita comprar un circuito telefónico local entre su sitio remoto y un punto de conexión cercano de Frame Relay. Después de ese punto, sus paquetes se entremezclan con los de cientos de otras empresas.

Por lo general, se requiere un dispositivo llamado FRAD para hablar a una red Frame Relay. FRAD (Frame Relay Assembler/Disassembler, ensamblador/desensamblador de Frame Relay), que analiza flujos de datos en el formato de paquetes apropiados de Frame Relay. El uso de un FRAD sólo lo conectan y le ofrece poco en la manera de administración remota, seguridad y calidad es servicio. Cisco ha construido capacidad de Frame Relay en muchos de sus enrutadores para proporcionar más inteligencia sobre conexiones Frame Relay. En la figura 14-15 se muestra una configuración típica de Frame Relay que usan equipo de Cisco.

Debido a que Frame Relay usan conexiones de línea serial normales, no se requiere una interfaz especial en un enrutador para que sea compatible con Frame Relay. El enrutador Cisco 2600 es una solución costeable para las tiendas del ejemplo de la figura 14-15, porque

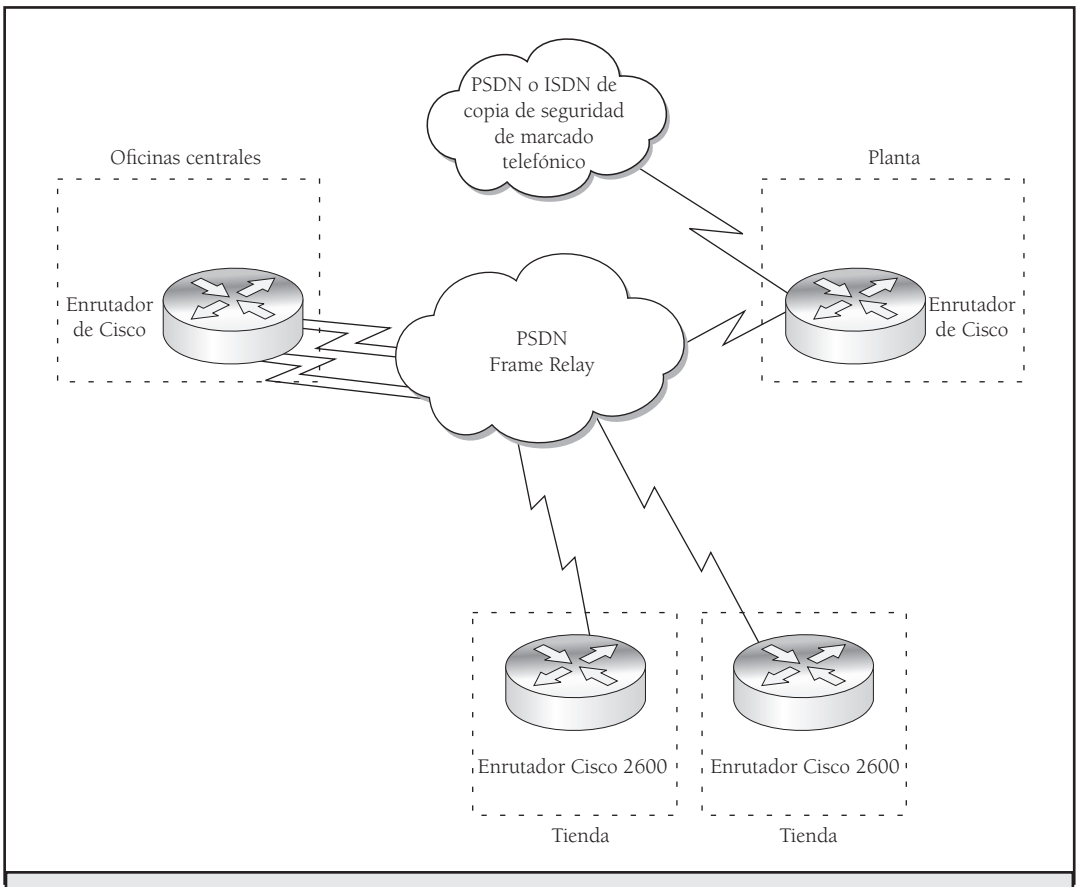


Figura 14-15. Los enrutadores con capacidad de Frame Relay son superiores a los FRAD para los vínculos de administración.

tienen suficiente capacidad de transmisión de datos para manejar las cargas de tráfico que es probable que estas locaciones remotas generen.

Red digital de servicios integrados Integrated Services Digital Network (ISDN) puede usarse para conexiones remotas de marcado telefónico o dedicadas. Proporciona mucho más ancho de banda que las conexiones electrónicas de modelo análogo normal, pero debe estar disponible en una portadora local para poder usarse. ISDN tiene opciones de canal llamadas BRI y PRI. BRI tiene dos denominados canales B para entregar un ancho de banda de 128 Kbps, y suele usarse para conexiones de marcado telefónico desde casa o pequeñas oficinas, o para copias de seguridad en caso de muchas fallas de conexión. PRI empaqueta 23 canales B, para un ancho de banda de alrededor de 1.48 Mbps, y suele usarse para conexiones de varios usuarios de tiempo completo. A esto suele denominarse como T1.

En la figura 14-16 se muestra una configuración ISDN típica de Cisco. Los enrutadores de la serie 800 de Cisco están dispuestos para conectarse a usuarios ISDN. El 836 tiene cuatro puertos y el 801 tiene un puerto. Como el 836 es capaz de manejar las necesidades de

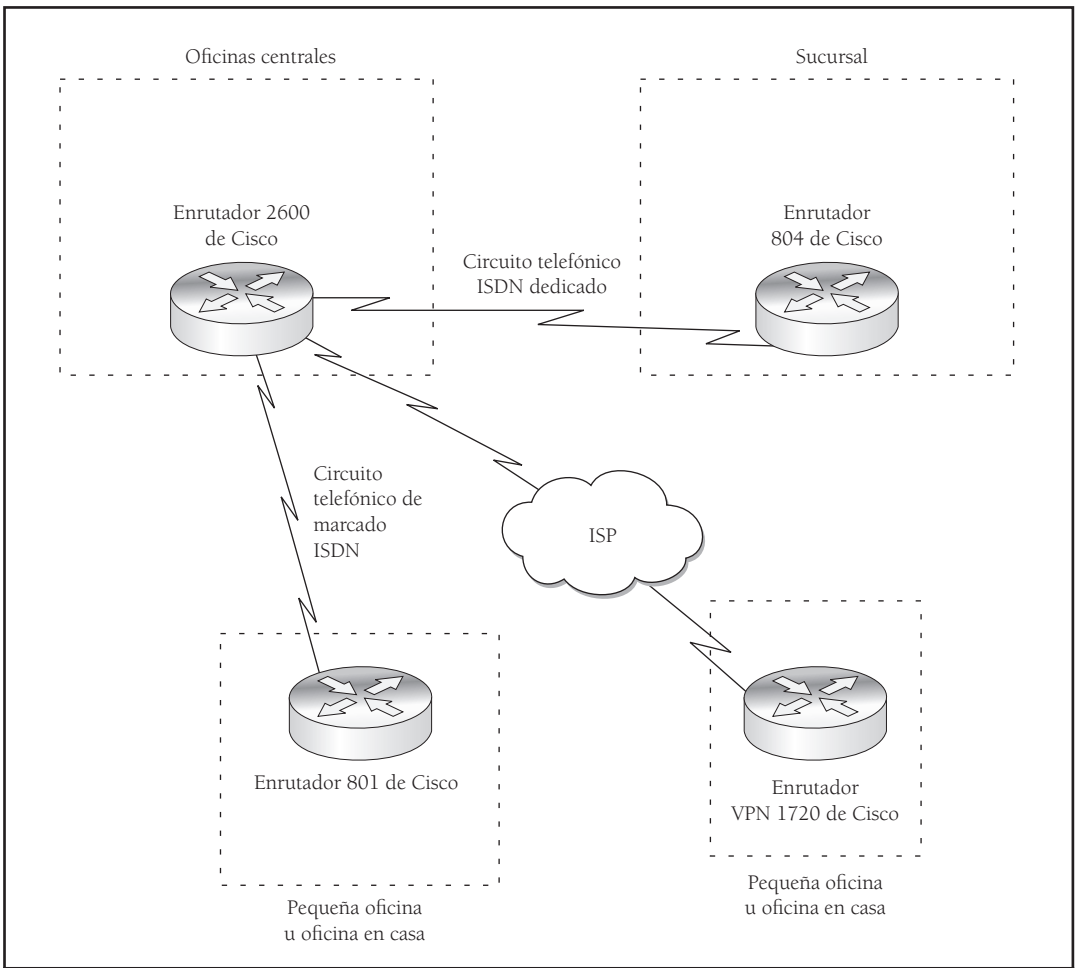


Figura 14-16. ISDN soporta conexiones de marcado telefónico y de circuito dedicado.

VPN, también se despliega como el enrutador en el área de la esquina inferior derecha de la figura 14-16. En este caso, el enrutador puede formar un túnel seguro a través de Internet.

Línea de suscriptor digital Digital Subscribir Line (DSL) está compitiendo con ISDN por el mercado de las pequeñas oficinas y oficina en casa. Para usar DSL, debe tener el servicio de parte de una oficina de conmutación telefónica local que soporte DSL y estar a cierta distancia de él (por lo general unos cuantos kilómetros).

Hay diferentes tipos de DSL, entre ellos incluyen:

- **ADSL** Caracterizado por las velocidades de datos asimétricas, donde más datos llegan de la compañía telefónica de los que el usuario puede enviar de regreso. Esto significa que ADSL debe usarse selectivamente donde las características del tráfico coinciden con esa restricción (en otras palabras, donde el usuario hace una

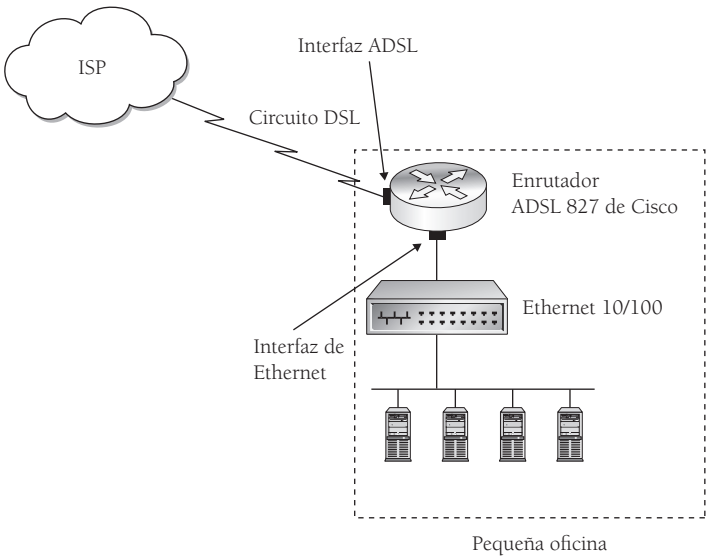


Figura 14-17. El enrutador ADSL 827 de Cisco es ideal para las conexiones DSL.

gran cantidad de descargas, pero no sube demasiada información). Sin embargo, ese es el caso de la mayoría de los usuarios de Internet y ADSL se ha vuelto muy popular donde las compañías telefónicas lo ofrecen.

- **SDSL** Caracterizado por las velocidades de datos simétricas, donde la misma cantidad de datos va en cualquier dirección. Ésta suele ser una solución más cara que ADSL.
- **IDSL** Una solución simétrica más lenta para lugares en que no están lo suficientemente cerca de una oficina de conmutación telefónica local, ofrece una velocidad máxima de transmisión de datos de 144 Kbps en ambas direcciones.

En la configuración de la figura 14-17 se muestra un enrutador ADSL (Asymmetric Digital Subscriber Line, línea de suscriptor digital asimétricas). El Cisco 837 parece un decodificador de televisión por cable, pero tiene una interfaz Ethernet en la parte trasera para conectar a los usuarios locales.

CAPÍTULO 15

Detección y solución de problemas en redes de Cisco

Mantener funcionando una interconexión es un trabajo de tiempo completo. Como ya lo vio, los problemas surgen con tal frecuencia que la industria inventó protocolos de enrutamiento para tratar con ellos de manera automática, sin esperar siquiera que el administrador de red intervenga. Hacen un buen trabajo, al menos con los problemas que pueden aminorarse al dar un rodeo para ir a una nueva ruta. Pero el cambio de rutas es sólo una solución temporal. Para que una red se ejecute de manera eficiente, todos sus componentes deben estarse ejecutando de manera apropiada y constante. Después de todo, entregar ancho de banda disponible a los usuarios bajo circunstancias normales es lo suficientemente difícil sin tener un segmento LAN fuera de la comisión o un enrutador funcionando a capacidad parcial.

Por esta razón, una gran parte del tiempo del equipo de una red se dedica a detectar y solucionar problemas. Éstos van desde un solo usuario que no puede acceder a un servicio hasta una falla en todo un segmento LAN. La detección y solución de problemas no se concreta a encontrar y corregir partes dañadas; gran parte de ella está dedicada a corregir los cuellos de botella del rendimiento. Cuando surge un problema, el administrador de red a menudo no tiene idea de cuál dispositivo lo está causando. Una vez que se ha identificado el dispositivo problemático, la causa del problema debe diagnosticarse. Luego deben tomarse decisiones sobre la manera de corregir la situación.

Debe aplicarse un método para la detección y solución de problemas; de otra manera, puede desperdiciarse una gran cantidad de tiempo tratando de descubrir qué es lo que está causando el problema. Como un doctor, la persona que intente solucionar los problemas debe reconocer los síntomas, asociados con un conjunto de probables causas y luego estrechar progresivamente la lista hasta que finalmente se identifique al culpable. A partir de allí, debe lidiarse e incrementarse un plan apropiado de acción. Ésa es la detección y solución de problemas.

En este capítulo, revisaremos la manera de detectar y solucionar problemas en diferentes configuraciones de Cisco al ejecutar algunos escenarios problemáticos. Para mayor simplicidad, supondremos que IP es el protocolo de red y que la plataforma Microsoft Windows es el host. Aunque la terminología puede variar, los problemas de red son muy parecidos, sin importar el protocolo en un entorno del host. También restringiremos los ejemplos a la detección y solución de problemas de enrutadores, que es donde generalmente hay más acción.

LA MECÁNICA DE LA DETECCIÓN Y SOLUCIÓN DE PROBLEMAS EN REDES

En las interconexiones, el problema suele ser causado por la falla de un dispositivo de hardware o puede tratarse de un problema de configuración. La ubicación de casi todos los problemas puede identificarse de manera remota, y en cierta medida, también pueden diagnosticarse los problemas e incluso corregirse remotamente (porque el hardware aún debe estar ejecutándose para que eso suceda). Por "corregir remotamente" nos referimos a que no iremos caminando e inspeccionaremos y tocaremos el dispositivo; no necesariamente significa que se quitará geográficamente. Si, digamos, la interconexión de campus de una empresa está experimentando un problema, los administradores de red por lo general harán la mayor parte de las tareas de detección y solución de problemas sin siquiera dejar sus escritorios.

En los entornos de Cisco, el trabajo remoto puede hacerse a través de una consola de administración de red, o al iniciar sesión directamente en el entorno de línea de comandos del IOS del dispositivo a través de Telnet o Secure Shell (SSH). Como ya aprendió, las consolas NMS de Cisco (CiscoWorks Resource Manager Essentials o CiscoWorks Campus Manager) usan sus interfases gráficas para manipular indirectamente los comandos IOS dentro del dispositivo remoto. Por tanto, casi todo el trabajo real de detección y solución de problemas tiene lugar dentro del entorno IOS del dispositivo. He aquí los principales comandos IOS para realizar la mayor parte de las tareas de detección y solución de problemas:

- **ping** Indica si los paquetes de "eco" están alcanzando un destino y regresan. Por ejemplo si ingresa **ping 10.1.1.1**, IOS regresará el porcentaje de paquetes que hizo eco de regreso desde la interfaz 10.1.1.1.
- **traceroute** Informa la ruta real tomada a un destino. Por ejemplo, si ingresa **traceroute ip 10.1.1.1**, IOS presentará una lista con cada salto que da el mensaje, hasta llegar a su destino en la interfaz 10.1.1.1.
- **show** Informa la configuración y estatus de los dispositivos por ejemplo, el comando **show memory** despliega cuanta memoria se está asignando a cada dirección de red y cuando queda libre.

El origen de los problemas debe estar en un dispositivo por un medio de red (cableado, conectores, etcétera). Aunque el problema sea en un cable, la manera de ir a él es a través de IOS. Los comandos **ping** y **trace** se usan para localizar problemas. Si el dispositivo aún se está ejecutando, los comandos **show** y **debug** se emplean para diagnosticarlos. Las conexiones reales se hacen al cambiar el hardware o su configuración. El comando **debug** es similar a **show**, con la excepción de que genera información mucho más detallada sobre las operaciones de los dispositivos (tanta que la ejecución de **debug** puede hacer mucho más lento el rendimiento del dispositivo).

Métodos para detección y solución de problemas en redes

Por lo general, los usuarios llaman la atención de los administradores de red sobre los problemas. Quieren saber por qué no pueden acceder a un servicio dentro de la interconexión de la empresa o se quejan de que el desempeño es lento. La ubicación y la naturaleza de la queja, son en sí mismas fuertes pistas sobre lo que está causando el problema. Muchas veces, el administrador sabe de inmediato lo que está mal y cómo corregirlo, pero en ocasiones debe lanzarse una investigación para descubrir qué dispositivo es el origen del problema, qué lo está causando y cuál es la mejor manera de corregirlo. El administrador de red debe encontrar respuestas al hacer una detección y solución de problemas metódica. Como podrá imaginar, esto funciona en gran medida a través de un proceso de eliminación, como en la siguiente lista:

- **¿Cuáles son los síntomas?** Por lo general, eso se reduce a que los usuarios no puedan llegar a un destino. Conocer ambos extremos de un problema de red (las direcciones de origen y destino) es la información de base en casi todas las situaciones de detección y solución de problemas.
- **¿Dónde debo empezar a mirar?** ¿El escenario se ajusta a un patrón conocido que sugiere causas probables? Por ejemplo, si el servidor no está respondiendo a las solicitudes de servicios de un cliente, podría haber un problema con el servidor o

con el propio del cliente. Si el servidor está trabajando bien para los demás clientes, entonces tal vez sea el dispositivo de cliente. Si no es así, entonces el problema debe residir en algún lugar entre los dos.

- **¿Dónde empiezo?** Hay reglas generales que hacen una lista corta de lo que es más probable que esté causando cierto tipo de síntomas. El administrador debe diagnosticar primero las causas que son "los mejores candidatos". Por ejemplo, si un servidor accedido en un vínculo WAN parece lento para los usuarios de marcado telefónico, es probable que el vínculo tenga algún problema, que se esté usando demasiado, que la interfaz del enrutador que sirve el vínculo se haya quedado sin memoria para el búfer o que los hosts estén mal configurados. Una de estas probables causas explicará el problema el 95% de las veces.
- **¿Cuál es el plan de acción?** Encontrar la causa exacta de un problema en un dispositivo que funciona mal, significa tratar con una variable en el tiempo. Por ejemplo, no tendría sentido reemplazar todos los módulos de la interfaz de red en un enrutador antes de reiniciar. Al hacerlo así se podría corregir el problema, pero no definiría el origen exacto o incluso lo que se corrigió. En la ciencia, a esto se le denomina cambiar una variable en el tiempo. La mejor práctica es concentrarse en el origen al reducir las variables de una en una. De esa manera, podría replicarse el problema, validar que la corrección es la adecuada y registrar la causa exacta para referencia futura. Un plan de acción también le permite deshacer cambios que no corrigen el problema (o que incluso lo empeoran).

NOTA Antes de adentrarse a tratar de aislar el problema al revisar direcciones IP u otra información de configuración, revisen los cables. Tal vez se ahorraría horas de problemas y esfuerzos al reconectar un cable suelto o un cable de alimentación de energía eléctrica que ha quedado inservible.

La mayor parte de los problemas de interconexiones se manifiestan con un rendimiento seriamente degradado o como mensajes de que se ha superado el tiempo máximo de espera debido a que "el destino es inalcanzable". En ocasiones, el problema es extenso; otras veces, está limitado a un segmento LAN o incluso a un host específico. Echemos un vistazo a algunos problemas típicos relacionados con sus causas probables. En la tabla 15-1 se delinean

Síntomas	Causas probables
El host no puede tener acceso a la red más allá del segmento LAN local.	Parámetros mal configurados en el dispositivo host, como una dirección IP de gateway predeterminada errónea o una mala máscara de subred.
	El enrutador de gateway no está funcionando bien.
El host no puede accesar a ciertos servicios más allá del segmento LAN local.	Lista de acceso extendida mal configurada en un enrutador entre el host y el servidor. Firewall mal configurada, si el servidor está más allá del sistema autónomo.
	Tal vez la propia aplicación esté fallando.

Tabla 15-1. Problemas críticos de acceso a host y causas.

Síntomas	Causas probables
Casi ningún usuario puede acceder a un servidor.	Especificación de gateway predeterminada mal configurada en el servidor remoto.
	Lista de acceso mal configurada en el servidor remoto.
	Los hosts no pueden obtener direcciones IP a través de DHCP.
No pueden hacerse conexiones a un área cuando una ruta se ha caído.	El protocolo de enrutamiento no converge dentro del dominio de enrutamiento.
	Todas las interfases en el enrutador que manejan una ruta alterna no se configuraron con direcciones IP secundarias (direccionamiento no continuo).
	Rutas estáticas configuradas de manera incorrecta.

Tabla 15-2. Problemas y causas comunes de enrutadores.

problemas con la colectividad de host. (Los hosts suelen ser PC de un solo usuario, pero no siempre.)

Por desgracia, casi ningún problema de interconexión se limita a un solo host. Si existen problemas en un enrutador o se dispersa a través del área, muchos usuarios y servicios se verán afectados. En la tabla 15-2 se delinean un par de problemas típicos de red que son los más extendidos.

Muchas veces, las redes y los servicios son alcanzables, pero el rendimiento es inaceptablemente lento. En la tabla 15-3 se presentan factores que pueden afectar el rendimiento dentro de una red local. Sin embargo, no tienen vínculos WAN. Se cubrirán por separado más adelante en este capítulo, porque las líneas seriales incluyen un conjunto ligeramente diferente de tecnologías y problemas.

Síntomas	Causas probables
Mala respuesta del servidor; es difícil establecer y mantener conexiones.	Vínculo de red erróneo, por lo general causado por un mal funcionamiento del módulo de interfaz de red o del medio de segmento LAN.
	Listas de accesos no coincidentes (en interconexiones de malla con múltiples rutas). Vínculo congestionado, saturado por demasiado tráfico.
	Equilibrio de carga mal configurado (mediciones de protocolo de enrutamiento).
	Configuraciones de velocidad o dúplex mal configuradas.

Tabla 15-3. Problemas y causas de rendimiento en LAN de campus.

Detección y solución de problemas de IP de host

Si un usuario está teniendo problemas al acceder servicios y la red general parece estar bien, un buen lugar para empezar a mirar la causa del problema es dentro de la computadora de la persona. Hay un par de cosas que podrían estar mal configuradas en la computadora host del usuario:

- **Información incorrecta de IP** La dirección IP o la información de la máscara de subred puede faltar o ser incorrecta.
- **Gateway predeterminada incorrecta** El enrutador de gateway determinado puede estar mal configurado.
- **Resolución de nombres que no están funcionando** Es posible que DNS o EINS estén mal configurados.

Para actualizar el tema, todos los hosts tienen una gateway predeterminada especificada en los parámetros de la red del hosts. Una gateway predeterminada es una interfaz en un enrutador local que se usa para pasar mensajes enviados por el host a dirección que están más allá de la LAN. Una gateway predeterminada (también denominada gateway de último recurso) está configurada, porque tiene sentido para un enrutador manejar casi todo el tráfico saliente del host para mantenerlo en una caché actualizada con direcciones IP de destino y rutas a ellas. Un host debe tener por lo menos una gateway, y en ocasiones una segunda se configura para redundancia en caso de que la primera gateway falle.

Revisión de información de dirección IP del host

Los parámetros de red mal configurados en los hosts de escritorio suelen ser atribuibles a un error por parte del usuario final. Tenga en mente que (en computadoras de Windows por lo menos) los administradores y los usuarios avanzados pueden acceder fácilmente y modificar las configuraciones de red. Por ejemplo, para revisar la dirección IP del host en Windows XP, haga clic en el botón **Start** de la barra de menús, elija **Run**, escriba **cmd** y luego haga clic en **OK**. Esto abrirá la ventana del indicador de comandos de Windows. En el indicador de comandos, escriba **ipconfig/all** y luego oprima **<enter>**. Esto desplegará la configuración de dirección IP del host.

Si necesita configurar parámetros de dirección IP del host, eso se hace a través de la pantalla Network Properties. Por ejemplo, para acceder a las propiedades de red en Windows XP, haga clic en el botón **Start** de la barra de menús y luego elija **Connect To | Show All Connections**. A partir de la lista resultante de conexiones de red, haga clic con el botón derecho en el icono de red apropiado, y luego seleccione **Properties**. Haga clic en la ficha **General** y en el cuadro This Connection Uses the Following Items, haga clic en **Internet Protocol (TCP/IP)** y luego haga clic en el botón **Properties**. En Windows NT/2000, haga clic en el botón **Start** de la barra de menús, y luego elija **Control Panel| Network | Configuration** y, por último, en **TCP/IP Properties**. Esto le permitirá establecer la dirección IP y la gateway predeterminada.

Por lo general el protocolo apunta a una Network Interface Card (NIC, tarjeta de interfaz de red) que conecta el host a la LAN, como en el caso de la tarjeta PC Ethernet TCP/IP resaltada en la figura 15-1. (Si el host se conecta por marcación telefónica a una interconexión, el protocolo que apunta al adaptador de marcado telefónico del estado estará seleccionado.)

Una vez que ya ha señalado a la NIC correcta, empiece por asegurarse que el host está identificándose asimismo de manera correcta en la red. En el ejemplo de la figura 15-2 se muestra una dirección IP y una subred definidas estáticamente. Eso debe coincidir con lo

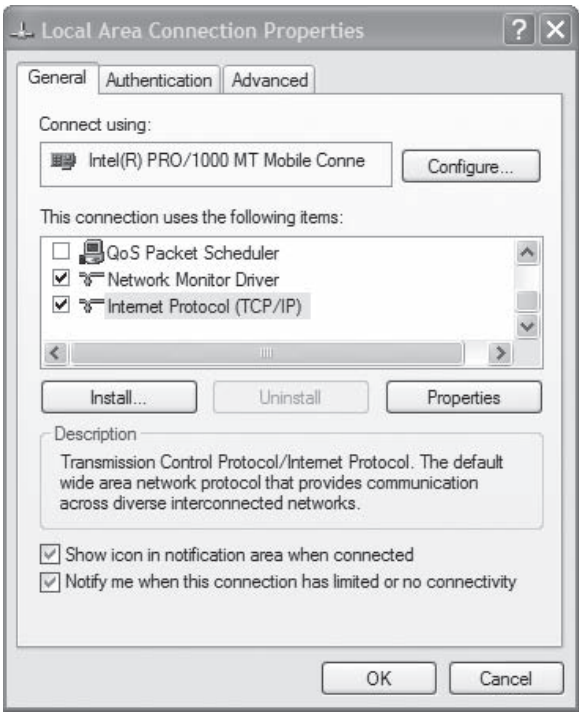


Figura 15-1. Para detectar y solucionar problemas de un host, el lugar para iniciar es la tarjeta de interfaz de red.

que se encuentra en el archivo del host en el archivo config del enrutador que da servicio a la gateway predeterminada. Si la casilla de verificación Obtain An IP Address Automatically está seleccionada, la dirección IP del host se asigna dinámicamente a través de un servidor Dynamic Host Control Protocol (DHCP, protocolo dinámico de control de host). Aunque DHCP puede facilitar la asignación de direcciones y es en cierto modo a prueba de tontos, los servidores DHCP falsos pueden ser problemáticos, de modo que asegúrese de revisar la configuración de la dirección IP para verificar cuál servidor DHCP está asignando a la dirección IP que usa el comando **ipconfig/all**.

A continuación, asegúrese de que la dirección IP declarada del host es la correcta al iniciar sesión en el enrutador de gateway e ingresar el comando **show arp**, recordará que ARP significa Address Resolution Protocol (protocolo de resolución de direcciones), una utilería que asigna la dirección de control de acceso a medios del dispositivo físico (capa 2) a su dirección IP asignada (capa 3) para manejar la etapa final de la entrega entre el enrutador de gateway y el host. En la figura 15-3 se muestra la tabla ARP en el archivo config de nuestro enrutador gateway de ejemplo. Las líneas sombreadas muestran que la interfaz Ethernet tiene una dirección 10.1.13.12 en el archivo, como se declara en la tabla de dirección IP del host. La dirección MAC también puede verificarse utilizando el comando **ipconfig/all**.

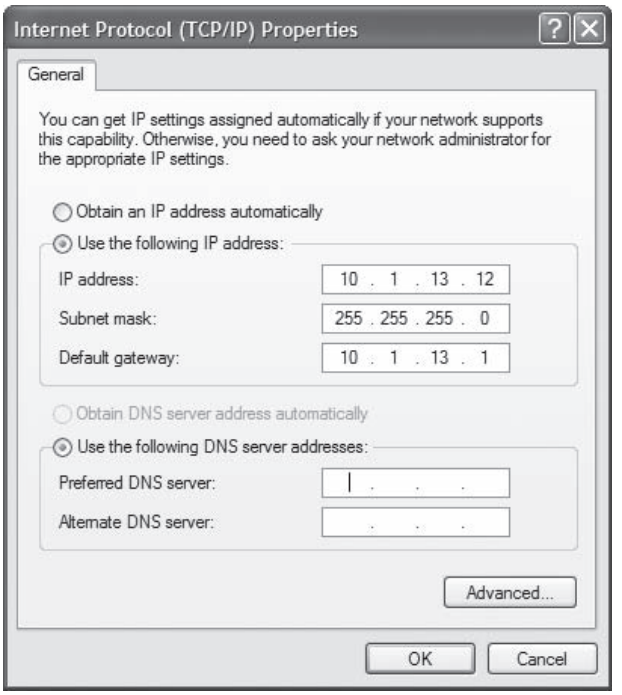


Figura 15-2. La configuración de la dirección IP del host y la de la gateway predeterminada deben coincidir.

Otro problema de host potencial es la configuración de la propia gateway predeterminada. En otras palabras, tiene que asegurarse de que el host tiene configurada la dirección IP correcta como su enrutador de gateway predeterminado, como se muestra en la figura 15-4.

La dirección IP de gateway predeterminada del host debe coincidir con la establecida para el módulo de interfaz de red en el enrutador de gateway. Para confirmar que esto es así, vaya al enrutador de gateway e ingrese el comando **show interfaces**, como se muestra aquí:

```
MyRouter#show interfaces
.
.
.
Ethernet1 is up, line protocol is up
 internet address is 10.1.13.1/28
 ip accounting output-packets
 ip nat inside
 ip ospf priority 255
```

Dirección MAC

```
vsigate#show arp
Protocol  address      Age (min)   Hardware Addr     Type   Interface

Internet  10.1.13.11       0       0050.0465.395c    ARPA   Ethernet1
Internet  10.1.11.1       12       0060.3eba.a6a0    SNAP   TokenRing0
Internet  10.1.13.12       9       00a0.c92a.4823    ARPA   Ethernet1
Internet  10.1.11.2        -       0006.f4c5.5f1d    SNAP   TokenRing0
Internet  10.1.11.3      190       0006.c1de.4ab9    SNAP   TokenRing0
Internet  10.1.12.3        -       0006.f4c5.5fdd    SNAP   TokenRing1
Internet  10.1.13.12      15       0050.04d7.1fa4    ARPA   Ethernet1
```

Figura 15-3. La dirección IP del hosts debe coincidir con la del enrutador de gateway en el archivo ARP.

```
media-type 10BaseT
.
.
.
```

Como puede ver, nuestra interfaz de ejemplo, Ethernet1, tiene la dirección 10.1.13.1, como se declaró en la ficha Gateway del host.

También es aquí donde puede revisar para asegurarse que la máscara de subred declarada del host coincide con la que se encuentra en el archivo del enrutador de gateway. La máscara/28 también correcta, porque coincide con la declarada en la ficha IP Address del host (255.255.255.240).

Obviamente, si ningún otro parámetro de red del host es incorrecto, el administrador debe ajustarlos para que coincidan con los parámetros del enrutador de gateway, reiniciar la PC y tratar de establecer una conexión de red. Por otra parte, si la configuración de la PC es correcta, quien hace la detección y solución de problemas debe trabajar fuera del host operable para identificar el origen del problema.

Aislamiento de problemas de conectividad

Casi todos los problemas de red se relacionan con la incapacidad de conectarse a un host o un servicio deseado. Los problemas de conectividad (también denominados "problemas de accesibilidad") se presentan de muchas maneras, como la terminación por alcanzar el tiempo de espera máximo de las conexiones HTTP que se intentan, conexiones de terminal intentadas que no obtienen respuesta del host, etcétera. Como se acaba de delinear, la persona que realiza la detección y solución de problemas primero debe asegurarse de que el host que informa el problema esté configurado de manera adecuada, y luego trabajar hacia

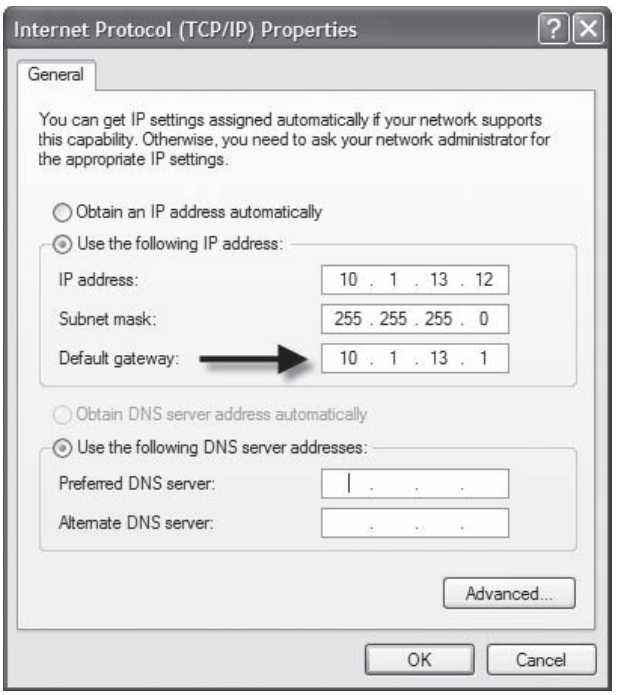


Figura 15-4. Asegúrese de que esté configurada la dirección IP de gateway predeterminada correcta.

fuera. Para dibujar una analogía, esta persona debe trabajar en el vecindario de puerta en puerta de manera muy parecida a como un policía en busca de pistas.

Revisión entre el host y su enrutador de gateway

Si los parámetros de red del host están configurados adecuadamente, el siguiente paso consiste en trabajar hacia fuera del host al enrutador de gateway. Esto debe hacerse aunque el problema del host sea la falla en conectarse un servidor remoto. Antes de trabajar mucho más lejos, la mejor práctica es primero revisar el vínculo entre el host y su enrutador de gateway.

Uso del comando ping La manera más fácil de revisar un vínculo es usar el comando **ping**, este comando envía paquetes de reconocimiento a un dispositivo de red específico para ver si es alcanzable. En términos técnicos, **ping** envía sus paquetes a través del protocolo de transporte ICMP en lugar de hacerlo a través de UDP o TCP. En realidad envía varios paquetes, como se muestra aquí:

```
MyRouter#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
MyRouter#
```

Las computadoras de host y los dispositivos de red tienen comandos **ping**. El ejemplo anterior fue tomado del enrutador Cisco, y el ping alcanzó con éxito a su destino. Pero también podría usarse el comando **ping** disponible en la línea de comandos del host. Estamos usando un host de Windows para nuestros ejemplos, pero otras plataformas (como las marcas, las diversas plataformas Unix, OS/400 de IBM y otras arquitecturas de servidor de propietario) todas tienen **ping** y otros comandos básicos de red integrados en sus sistemas operativos.

Por lo general, la primera prueba de ping de un host es el vínculo a su enrutador de gateway. En una computadora que ejecuta Windows XP, revise esto al hacer clic en el botón **Start**, de la barra de menús y eligiendo **All Programs** \ **Accessories** \ **Command Prompt** para abrir una ventana de indicador de comandos. Luego revise para ver si el enrutador de gateway está respondiendo al ingresar el comando **ping**, como se muestra en el siguiente fragmento de código:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985–2001 Microsoft Corp.

C:\Documents and Settings\Tony>ping 10.1.13.1

Pinging 10.1.13.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.13.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Tony
```

El ejemplo anterior muestra que cuatro paquetes de ping fueron enviados al enrutador de gateway, que falló en responder. Esto indica a la persona que hace la detección y solución de problemas unas cuantas cosas:

- ▼ La NIC de la PC host está bien; de otra manera, el sistema operativo habría generado un mensaje de error cuando la tarjeta falló en responder al comando **ping**.
- ■ Es probable que un segmento LAN de Ethernet haya dejado de funcionar (una condición a la que a menudo se alude como un "problema de medios"). (El medio compartido aparentemente no está trabajando.)
- ▲ El módulo de interfaz de red en el enrutador de gateway tal vez esté fallando.

Si la revisión del host resulta correcta, la persona que hace la detección y solución de problemas debe avanzar hacia fuera. Como ya lo mencioné, la investigación debe empezar con el vínculo en el enrutador de gateway.

Ping extendido Aunque el comando **ping** es muy útil y utilitario para la detección y solución de problemas, tiene sus límites. Cuando se usa **ping**, la dirección de origen del **ping** es la dirección IP de la interfaz que el paquete usa tal como existe en el enrutador. Si necesita más precisión de su **ping**, puede actualizar al comando ***ping extendido***.

Ping extendido realiza una revisión más avanzada de la capacidad de su sistema para alcanzar un host particular. Este comando funciona sólo en la línea de comandos Privileged EXEC, mientras que un comando **ping** normal funciona en ambos modos, User EXEC y Privileged EXEC.

El uso del extended ping en enrutadores de Cisco es muy sencillo. Simplemente ingrese **ping** en el indicador de comandos y luego oprima Enter. Se le pedirá varias condiciones y variables. La configuración predeterminada aparece entre corchetes. Si le gustaría la opción predeterminada, simplemente oprima Enter; de otra manera, ingrese su opción preferida.

El siguiente listado muestra un ejemplo de un ping extendido en funcionamiento:

```
Router<>ping
Protocol [ip]:
Target IP address: 64.66.150.248
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sending 100, 100-byte ICMP Echos to 64.66.150.248, timeout is 2
seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 12/19/280 ms
```

NOTA El comando **ping** también existen en su propia forma en entornos de Windows y UNIX/LINUX. Simplemente agregue los conmutadores –s (UNIX/LINUX) o –t (Windows) después del comando **ping**.

Uso del comando show interfaces Para revisar si el problema es la interfaz del enrutador de gateway o un medio del segmento LAN, inicie sesiones del enrutador de gateway e ingrese el comando **show interfaces** para obtener el siguiente informe:

```
MyRouter#show interfaces
Ethernet1 is up, line protocol is down
  Hardware is MyRouter, address is 0060.2fa3.fabd (bia 0060.2fa3.fabd)
  Internet address is 10.1.13.1/28
  .
  .
  .
```

En el ejemplo anterior, el enrutador reporta que el módulo de interfaz de red Ethernet1 está funcionando y que el protocolo de la línea ha dejado de hacerlo. El término *protocolo de la línea* denota el cable en el enrutador y el protocolo LAN que se ejecuta en él. Un protocolo de la línea que se reporta como fallido probablemente indica que el medio compartido del

segmento LAN (un concentrador, un conmutador de acceso o un cable) está fallando. A partir de aquí, revisaría físicamente el medio para identificar el problema de hardware. (En páginas posteriores de este capítulo se cubrirá la manera de hacerlo, en la sección "Detección y solución de problemas del hardware de Cisco".)

Otra posible condición podría hacer que un administrador de red haya deshabitado la interfaz o la línea, o ambas. Esto se hace de manera rutinaria mientras una pieza de equipo se está reparando, actualizando o reemplazando. Notificar al IOS que una pieza del equipo ha dejado de funcionar por mantenimiento evita que se tengan mensajes innecesarios de error generados por el enrutador. En el siguiente ejemplo se muestra el reporte cuando un módulo de interfaz de red ha dejado de funcionar por razones administrativas:

```
MyRouter#show interfaces
Ethernet1 is administratively down, line protocol is down
  Hardware is MyRouter, address is 0060.2fa3.fabd (bia 0060.2fa3.fabd)
  Internet address is 10.1.13.1/28
  .
  .
  .
```

Si una pieza del equipo ha dejado de funcionar por diseño o por un mal funcionamiento, aún detiene el tráfico. De modo que es importante saber cuándo la pieza del equipo está funcionando en orden para asegurarse de que esté disponible una ruta alterna para manejar el tráfico.

Si la interfaz del enrutador gateway y el protocolo de línea están funcionando bien, la causa del problema de conectividad probablemente reside en un vínculo con otra red.

Detección y solución de problemas de conexión a otras redes

Las cosas se complican un poco más allá del segmento LAN de origen. Si el host no se puede conectar más allá del enrutador de gateway, hay a la vez más orígenes posibles y más tipos de problemas que revisar. Lo que significa *orígenes* de problemas posibles aquí, es que muchos más dispositivos de hardware deben considerarse como causas posibles del problema de accesibilidad. Lo que significa tipos de problemas posibles es que cosas como listas de acceso, protocolos de enrutamiento y otros factores más allá del hardware deben ahora tomarse en consideración.

Uso del comando trace para detectar zonas problemáticas En lugar de hacer ping hacia fuera desde el shocks de vínculo en vínculo, la ruta entre el host y el servidor inalcanzable puede analizarse de una sola vez utilizando el comando **trace route**. En nuestro ejemplo el host de Windows, esto se hace al elegir **Start | Run**, y luego escribir **cmd** para acceder al indicador de comandos. Una vez allí, ingrese el comando **tracrt**, la versión de Microsoft del comando **trace route**. En el ejemplo de la figura 15-5 se muestra la ruta que se está tratando desde la PC host hasta www.PayrollServer.AcmeEnterprises.com, que es un servidor interno ficticio que se encuentra a varios saltos de distancia. Es opcional usar el nombre de dominio o la dirección IP. Cada línea del comando **tracert** representa un salto a lo largo de la ruta hacia el destino.

En interconexiones TCP/IP, los comandos **trace route** funcionan al enviar tres paquetes de "rastreo" a cada enrutador tres veces y registrar los tiempos de respuesta del eco. Al igual

```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>tracert www.PayrollServer.AcmeEnterprises.com

Tracing route to www.PayrollServer.AcmeEnterprises.com [10.1.22.19]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  10.1.13.12  <---- Enrutador de gateway del host
  2   <10 ms    12 ms   <10 ms  10.1.5.3
  3    17 ms    20 ms    19 ms  10.1.17.22
  4    22 ms    19 ms    23 ms  10.1.31.2
  5   768 ms   831 ms   790 ms  10.1.49.12  <---- La respuesta lenta indica que
  6    31 ms    40 ms    42 ms  10.1.22.19        es probable que este enrutador
                                                   sea culpable.

Trace complete.

C:\>
```

Figura 15-5. El comando **trace route** es una manera estupenda de detectar el origen de un problema.

que con el comando **ping**, los paquetes usan el protocolo de transporte ICMP. Sin embargo, estos paquetes difieren de los paquetes ping en que tienen un campo Time-To-Live (TTL, tiempo de vida) usado para aumentar hacia fuera del host un paso cada vez. El campo TTL causa que el paquete muera cuando el contador llega a cero. El comando **trace route** usa el campo TTL al enviar el primer paquete de rastreo al enrutador más cercano con un TTL de uno, al siguiente enrutador con un TTL de dos, etcétera. Ese proceso se repite hasta que se alcanza el host de destino (si es alcanzable) el administrador de red puede poner un límite sobre el número de saltos que el rastreo puede dar automáticamente para detener el proceso si se prueba que el destino es inalcanzable.

Las lecturas *ms* son milisegundos, y puede ver que los enrutadores cercanos naturalmente tienden a tener un eco más rápido. Debajo de 10 ms es rápido; cualquier cosa arriba de 100 ms se está volviendo lento (pero siempre debe de ajustar los tiempos de acuerdo con el número de saltos al que se encuentra el enrutador). Como puede ver, el enrutador en la línea sombreada de la figura 15-5 es el probable sospechoso del servicio lento debido a sus tiempos de respuesta lentos. La explicación probable es que la interfaz del enrutador o el segmento LAN adjunto a él está congestionado o está experimentando falla de hardware. El siguiente paso sería utilizar Telnet en el enrutador 10.1.49.12 (si es posible) y diagnosticar el sistema, la interfaz de red relacionada, etcétera. Si no es posible establecer una conexión Telnet, la persona encargada de la detección y solución de problemas debe ir al puerto Console o AUX que, por supuesto,

requiere que alguien esté físicamente presente en el dispositivo, a menos que se haya configurado de antemano una solución de mantenimiento de marcado telefónico.

En ocasiones, un trace route localizará un nodo que está deteniendo el tráfico por completo. Un ejemplo de esto se muestra en la figura 15-6, donde 10.1.49.12 ahora están eliminando los paquetes de rastreo en lugar de simplemente regresarlos lentamente. Los asteriscos indican un resultado de tiempo nulo porque no regresa nada, y el mensaje "request timed out" está insertado. Tomen nota de que no necesariamente significa que todo el enrutador haya dejado de funcionar. Puede ser que sólo la interfaz de red o el segmento LAN que conecta al enrutador sospechoso haya dejado de funcionar o no esté configurado para responder ping.

```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>tracert www.PayrollServer.AcmeEnterprises.com

Tracing route to www.PayrollServer.AcmeEnterprises.com [10.1.22.19]
over a maximum of 15 hops:

  1   <10 ms   <10 ms   <10 ms  10.1.13.12
  2   <10 ms    12 ms   <10 ms  10.1.5.3
  3    17 ms    20 ms    19 ms  10.1.17.22
  4    22 ms    19 ms    23 ms  10.1.31.2
  5     *        *        *     request timed out
  6     *        *        *     request timed out
  7     *        *        *     request timed out
  8     *        *        *     request timed out
  9     *        *        *     request timed out
 10     *        *        *     request timed out
 11     *        *        *     request timed out
 12     *        *        *     request timed out
 13     *        *        *     request timed out
 14     *        *        *     request timed out
 15     *        *        *     request timed out

Trace complete.

C:\>
```

El comando trace route del host está establecido para detenerse después de 15 saltos en este ejemplo.

Esta vez, el host no pudo alcanzar a 10.1.49.12.

Cada rastreo fallido a 10.1.49.12 se cuenta contra el límite de 15 saltos.

Figura 15-6. He aquí lo que sucede si una ruta trazada encuentra que un enrutador detiene el tráfico.

Si es posible, primero trate de utilizar Telnet en el enrutador a través de una de sus otras interfaces. Si esto no funciona, la siguiente movida depende de la proximidad al enrutador. Si está cercano, vaya a él y regístrese a través del puerto Console o AUX. Si es remoto, debe ponerse en contacto con la persona responsable de hacer el marcado telefónico y hacer que la persona recorra los pasos del diagnóstico.

NOTA La detección y solución casi siempre toma lugar dentro de una interconexión entre la interconexión de la empresa. Esto se debe a que el equipo de red puede controlar eventos sólo dentro de su sistema autónomo. El comando **trace route** es un buen ejemplo de esto. Si rastrea una ruta a través de Internet (digamos, para detectar y solucionar problemas de la conexión VPN) muchas líneas entre su enrutador de gateway y el nodo de destino le volverán asteriscos en lugar de tiempos y mensajes "request time out" en lugar de direcciones IP. Esto se debe a que casi todos los enrutadores de orilla están configurados por sus equipos de red para no responder a **trace route**. Esto se hace como precaución de seguridad. Lo importante aquí es destacar el equilibrio que debe tener una VPN. La pérdida de control se intercambia por el bajo costo de los vínculos WAN; por lo general no puede detectar y solucionar problemas en las redes de alguien más.

Uso del comando show interfaces Una vez que el módulo de interfaz de red sospechoso sea identificado, la persona que se encarga de la detección y solución de problemas debe diagnosticar lo que está causando el problema. La mejor manera de hacerlo es ejecutando el comando **show interfaces** y revisar las últimas estadísticas sobre las operaciones de la interfaz. Recuerde que su información no sólo se refleja en el propio módulo de la interfaz, sino que también da un conjunto rico de pistas sobre lo que está sucediendo fuera de la red.

Un ejemplo de informe de **show interfaces** se da en la figura 15-7. No deje que su tamaño y su terminología criptica lo intimide. Por supuesto que aquí hay una gran cantidad de información, pero nada que requiera ser un científico espacial para comprenderlo.

Este informe es una instantánea de la interfaz en un instante particular en el tiempo. Para revisar las tendencias, la persona que hace la detección y solución de problemas debe ejecutar el comando **show interfaces** de manera intermitente para observar los cambios. La interfaz se identifica por la dirección IP privada 10.1.49.12/28. Recuerde que por lo general sólo los enrutadores en la orilla de un sistema autónomo (firewalls, servidores Web, servidores FTP, etcétera) usan direcciones públicas de Internet. La anotación /28 le permite a los otros enrutadores saber que los segmentos LAN adjuntos a RemoteRouter tienen la máscara de subred 255.255.255.240. La notación usa 28 porque la máscara 255.255.255.240 tiene 28 bits disponibles para direcciones de red (en oposición a los host). Como ya mencioné, las subredes que no coinciden a menudo causan problemas.

Lo primero que debe buscar es la séptima línea del reporte **show interfaces** que dice "Last clearing of show interfaces counters never" (resaltado en la figura 15-7). El ejemplo establece que nadie ha restablecido los contadores del informe a cero desde la última vez que el enrutador fue reiniciado. La duración desde que las estadísticas se limpiaron por última vez es importante, porque casi todas las estadísticas son números absolutos, no valores relativos, como porcentajes. En otras palabras, cuanto mayor sean los totales que ha compilado IOS, menos peso se le debe dar a las estadísticas. Por ejemplo, diez exportadoras perdidas en un día son muchas, pero el mismo total en seis meses no lo es. Para ver cuándo fue el último reinicio, utilice el comando **show version**, como se muestra aquí.

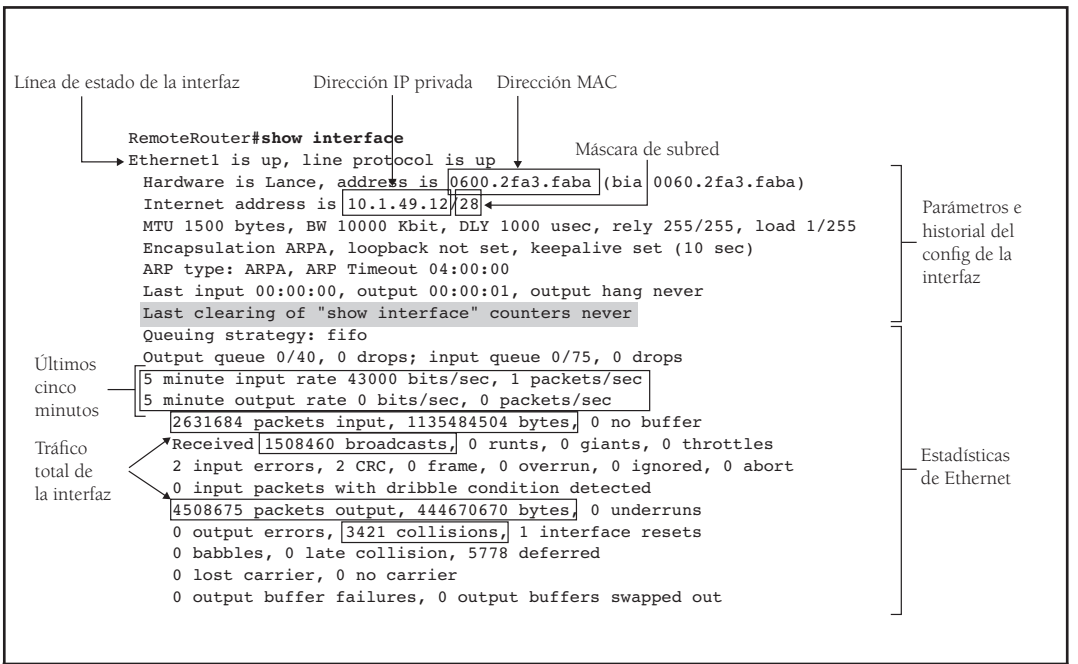


Figura 15-7. El comando **show interfaces** es una de las mejores herramientas para la detección y solución de problemas.

```
RemoteRouter#show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 11.2(17),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by Cisco Systems, Inc.
Compiled Mon 04-Jan-99 18:18 by etlevynot
Image text-base: 0x600088A0, data-base: 0x60604000

ROM: System Bootstrap, Version 5.3(10) [tamb 10],
RELEASE SOFTWARE (fc1)
BOOTFLASH: 4500 Bootstrap Software (C4500-BOOT-M), Version 10.3(10),
RELEASE SOFTWARE (fc1)

RemoteRouter uptime is 2 weeks, 3 days, 13 hours, 32 minutes
System restarted by power-on
.
.
.
```

La penúltima línea del ejemplo anterior muestra que el enrutador ha estado activo por casi dos semanas y media. El saber esto le permite a la persona que hace la detección y solución de problemas juzgar de manera más exacta si ciertos tipos de errores son normales o excesivos.

NOTA Históricamente, ha habido un amplio rango de problemas de interoperabilidad identificados entre diferentes versiones de IOS. Cuando se detectan y solucionan problemas, debe tomar nota de las versiones de IOS que se ejecutan en el entorno y evaluar el impacto de la ejecución de diferentes versiones.

La excepción de esta ventana de ejemplo son las dos líneas que se encuentran en la parte media de la figura 15-7. Éstas informan entrada y salida a la interfaz en los últimos cinco minutos antes de que sea ejecutado el informe. Una persona que hace la detección y solución de problemas que trate discernir una tendencia en los patrones de tráfico generará periódicamente el informe **show interfaces** y revisará estos números.

Las estadísticas difieren en lo que se considera excesivo. Por ejemplo, Ethernet arbitra el control de acceso a medios mediante condiciones, de modo que es normal para ellas que ocurran en algún grado en un entorno de medio compartido (uno con un concentrador por ejemplo). La cuenta de 3 421 coaliciones de la figura 15-7 es correcta para un periodo de dos semanas, pero una cifra de 50 000 sería un indicativo de un ancho de banda congestionado. Los paquetes de transmisión también son normales, porque realizan funciones positivas, como alertar a los enrutadores sobre los cambios en la topología y proporcionar otras actualizaciones útiles (de nuevo dentro de los límites). Hay más de un millón y medio en la figura 15-7, lo que podría ser excesivo. Sin embargo, lo que se considera excesivo es tema de muchas variables que deben dejarse a juicio de la persona que hace la detección y solución de problemas. Ahí es donde la experiencia entra en juego. Para un entorno conmutado configurado de manera apropiada, casi no debe haber condiciones en un solo puerto. Se están viendo condiciones, es muy posible que tenga una falta de coincidencia en velocidad o dúplex.

Muchas estadísticas idealmente deben ser bajas, o incluso estar en cero (dependiendo del periodo reportado). Por ejemplo, *enanos* y *gigantes* son paquetes malformados que a veces se deben a una receta de interfaz de red que está funcionando mal o una VLAN configurada de manera inapropiada. En un vínculo WAN, los eventos portadores perdidos probablemente indiquen una línea sucia o un componente de telecomunicaciones que está fallando.

En la tabla 15-4 se definen muchos de los elementos reportados usando el comando **show interfaces**. Al conocer los elementos le ayudará a comprender cómo pueden usarse para diagnosticar problemas.

Estadística	Explicación
Five-minutes rates (input o output)	El número promedio de bits y paquetes que pasan por la interfaz cada segundo, como aparecen en las muestras del último intervalo.
Aborts	Terminación súbita de paquetes de transmisión de un mensaje.
Buffer failures	Paquetes descartados por una falta de memoria disponible en el búfer del enrutador.
BW	Ancho de banda de la interfaz en kilobits por segundo (Kbps). Esto puede usarse como una medición de protocolo de enrutamiento.

Tabla 15-4. Definiciones de las estadísticas útiles de Ethernet (*continúa*).

Estadística	Explicación
Bytes	Número total de bits transmitidos a través de la interfaz.
Carrier transitions	Un portador es la señal electromagnética modulada por la transmisión de datos en líneas seriales (como el sonido que hace su módem). Las transiciones de portador son eventos donde la señal es interrumpida, a menudo causada cuando se restablece una NIC remota.
Collisions	El número de mensajes transmitidos debidos a una coalición de Ethernet.
CRC	Verificación de redundancia cíclica, o la técnica común para detección de errores de transmisión. CRC trabaja al dividir el tamaño del contenido de un marco por un número primo y compara lo que sobra con el almacenado en el marco por el nodo que envía.
DLY	Demorar el tiempo de respuesta de la interfaz, medido en microsegundos (µs), *no* en milisegundos (ms)
Dribble conditions	Marcos que son demasiado largos, pero que aún son procesados por la interfaz.
Drops	Número de paquetes descartados por una falta de espacio en la cola.
Encapsulation	El método de encarcelamiento asignado a una interfaz (si lo hay). Funcionan al envolver datos en el encabezado de un protocolo para "entunelar" datos que de otra manera serían incompatibles a través de una red externa. Por ejemplo, Inter-Switch Link (ISL) de Cisco encapsula marcos de muchos protocolos.
Errors (input y output)	Condición en que se descubre que una transmisión no coincide con lo que se esperaba, por lo general en relación con el tamaño de un marco o un paquete. Los errores se detectan usando varias técnicas como CRC.
Frame	El número de paquetes que tienen un error de CRC y un tamaño de marco parcial. Por lo general indican un mal funcionamiento de un dispositivo Ethernet.
Giants	Paquetes más grandes que el tamaño de paquete máximo de la tecnología LAN (1 518 bits o más en redes Ethernet). Todos los paquetes gigantes son descartados.
Ignored	Número de paquetes descartados por la interfaz por falta de memoria búfer disponible en la interfaz (en oposición a la memoria búfer del enrutador).

Tabla 15-4. Definiciones de las estadísticas útiles de Ethernet (*continúa*).

Estadística	Explicación
Interface resets	Cuando la interfaz se limpia a sí misma de todos los paquetes y empieza de nuevo. Por lo general los establecimientos ocurren cuando se lleva demasiado tiempo para que los paquetes esperados sean transmitidos por el nodo que envía.
Keepalives	Mensajes enviados por un dispositivo de red a otro para notificar que el circuito virtual entre ellos está activo.
Last input u output	Horas, minutos y segundos desde que se transmitió con éxito el último paquete o que la interfaz lo recibió. Una buena herramienta para determinar cuándo empezó el problema.
Load	La carga en la interfaz como fracción del 255. Por ejemplo, 64/255 es una carga de 25%. Este contador puede usarse como una medición de protocolo de enrutamiento.
Loopback	*Loopback* es donde las señales se envían desde la interfaz y luego se redirigen de regresó hacia ella desde algún punto de la ruta de comunicaciones; se usa para probar la utilidad del vínculo.
MTU	La unidad máxima de transmisión para paquetes que pasan a través de la interfaz, expresada en bytes.
Output hang	Cuánto tiempo ha pasado desde que se restableció la interfaz por última vez. Toma su nombre del hecho de que la interfaz "se cuelga" debido a que la transmisión toma mucho tiempo.
Overruns	El número de veces que la interfaz del enrutador satura el nodo receptor al enviar más paquetes de los que el búfer del nodo puede manejar. Toma su nombre del hecho de que la interfaz del enrutador "desborda" al remitente.
Queues (input y output)	Número de paquetes en la cola. El número detrás de la diagonal es el tamaño máximo de la cola.
Queuing strategy	FIFO (First In, Firts Out; primero en entrar, primero en salir) significa que el enrutador maneja paquetes en ese orden. LIFO (Last In, First Out, último en entrar, primero en salir) indica que esa es la estrategia seguida. FIFO la opcion predeterminada.
Rely	La confiabilidad de la interfaz como fracción del 255 por ejemplo, 255/255 es una confiabilidad de 100%. Ese contador puede usarse como medición de protocolo de enrutamiento.
Runts	Paquetes más pequeños que el tamaño de paquete mínimo de la tecnología LAN (64 bytes o menos en las redes Ethernet). Todos los paquetes enanos son descartados.

Tabla 15-4. Definiciones de las estadísticas útiles de Ethernet (*continúa*).

Estadística	Explicación
Throttles	El número de veces que la interfaz anuncia a la NIC que envía, que está saturada de paquetes que se están enviando y que reducen el ritmo del envío. Toma su nombre derecho de que la interfaz pide a la NIC que corte el envío.
Underruns	Es el número de veces que el nodo que envía satura la interfaz al enviar más paquetes de los que los búferes pueden manejar. Toma su nombre del hecho de que la interfaz del enrutador "subestima" al remitente.

Tabla 15-4. Definiciones de las estadísticas útiles de Ethernet (*conclusión*).

Ahora que hemos introducido las diferentes estadísticas compiladas en el informe **show interfaces**, revisemos cómo leerlo. En la figura 15-8 se muestra la parte de las estadísticas Ethernet del informe, esta vez con algunas de las variables más importante para resaltar. Éstas son las variables que un administrador de red con experiencia revisaría primero en busca de pistas.

Lo más frecuente es que los problemas de conectividad sean causados por algún tipo de problema de configuración, no por una pieza de equipo que falla. Dependiendo de las estadísticas de Ethernet que son altas, la interfaz puede estar saturada por tráfico entrante, tener configurado un tamaño de cola insuficiente, tener insuficiente memoria en el búfer o tener una falta de coincidencia con la velocidad de la entrada de envío de una red.

Revisión de las listas de acceso para una configuración apropiada El ejemplo clásico de un dispositivo que funciona mal aunque su hardware esté ejecutándose bien es la lista de acceso mal configurada. Recordará que las listas de acceso se usan para restringir el tráfico que puede pasar a través de la interfaz del enrutador, cortando así el acceso al segmento LAN adjunto. La lista de acceso hace esto al inspeccionar las direcciones IP de origen y destino (una manera de controlar quién podría ir a dónde). La lista de acceso extendida también usa números de puerto para restringir aún más cuáles aplicaciones pueden ejecutarse una vez que usted haya sido admitido. De hecho, las listas de acceso son la forma más rudimentaria de seguridad de interconexión, usadas como una especie de firewall interno. No todo el uso de las listas de acceso tiene que ver con la seguridad; en ocasiones se usan para dirigir el tráfico a lo largo de ciertas rutas para dar "forma" al tráfico de modo que se ajuste mejor a los recursos de la interconexión.

El primer paso en la revisión de los problemas de lista de acceso consiste en determinar si un enrutador sospechoso (o interfaz sospechosa en un enrutador) está configurado con una lista de acceso. Para saber esto, inicie sesión en el enrutador y luego ingrese el comando **show access-lists** para ver si todas las listas de acceso están configuradas:

Tamaño de cola de salida configurado muy por abajo del normal, con memoria de búfer del enrutador demasiado pequeña.

Tamaño de cola de entrada configurado muy por abajo del normal, con memoria de búfer del enrutador demasiado pequeña.

NIC que funciona mal en el dispositivo que envía.

```
Output queue 0/40, 7203 drops; input queue 0/75, 3923 drops
  5 minute input rate 43000 bits/sec, 62 packets/sec
  5 minute output rate 41000 bits/sec, 60 packets/sec
     2631684 packets input, 1135484504 bytes, 0 no buffer
     Received 1508460 broadcasts, 5673 runts, 4533 giants, 2343 throttles
     2 input errors, 2 CRC, 987 frame, 345 overrun, 678 ignored, 125 abort
     0 input packets with dribble condition detected
     4508675 packets output, 444670670 bytes, 1276 underruns
     0 output errors, 3421 collisions, 1 interface resets
     76 babbles, 567 late collision, 5778 deferred
     0 lost carrier, 0 no carrier
     146 output buffer failures, 0 output buffers swapped out
```

Velocidades de interfaz que no coinciden.

La interfaz, el enrutador, o ambos están congestionados.

Ancho de banda de segmento LAN sobreutilizado.

Figura 15-8. Cada elemento de interfaz probablemente tiene razones para que sus estadísticas sean altas.

```
RemoteRouter#show access-lists
Extended IP access list 100
    deny   ip any host 206.107.120.17
    permit ip any any (5308829 matches)
Extended IP access list 101
    permit tcp any host 209.98.208.33 established
    permit udp host 209.98.98.98 host 209.98.208.59
    permit icmp any host 209.98.208.59 echo-reply
    permit tcp any host 209.98.208.59 eq smtp
    permit tcp any host 209.98.208.59 eq pop3
    permit tcp any host 209.98.208.59 eq 65
    permit tcp any host 209.98.208.59 eq telnet
    permit tcp host 209.98.208.34 host 209.98.208.59
    permit tcp any 209.98.208.32 0.0.0.15 established
    permit icmp any 209.98.208.32 0.0.0.15 echo-reply
.
.
.
```

Al observar el ejemplo anterior, la lista de acceso 100 niega explícitamente el tráfico a una cierta dirección IP. Esto se hace frecuentemente para detener el tráfico saliente a una dirección IP indeseable o algún otro tipo de enrutador que pudiera permitir que los hackers ingresen en el enrutador de orilla de la empresa. La lista de acceso 101 es más compleja, con una serie de reglas de permiso para controlar cuáles aplicaciones pueden usarse entre los hosts. El puerto IP de la aplicación está definido detrás de cada modificador **eq**, como **eq smtp** para correo electrónico o **eq 65** para servicio de base de datos TACACS+. (Ciertos puertos pueden identificarse por un acrónimo; otros deben identificarse por un número.) Además, observe que la lista de acceso 101 sólo tiene reglas de permiso. Esto es posible porque si una solicitud de servicio de un paquete no está explícitamente permitida, será denegada por la regla de "negación implícita" cuando alcance la parte inferior de la lista de acceso.

Podría ser que la regla de negación inadvertida, la regla de permiso o un simple error de mecanografía lo que esté causando el problema. La persona que realiza la detección y solución de problemas revisaría las listas de acceso en busca de cualquier regla que pudiera causar el problema a mano. Por ejemplo, si una persona no puede conectarse a un servidor de correo, la persona que detecta el problema buscaría instrucciones que contengan **eq smtp** o la dirección IP del servidor de correo. El siguiente paso sería ir a la interfaz que conecta a la red que experimenta el problema para ver si el comando **access-group** se usó para aplicar la lista de acceso cuestionable a él. Para ello, debe ingresar en el modo Privileged EXEC y entrar en el modo de interfaz de configuración apuntado a la interfaz en cuestión, como se muestra aquí:

```
MyRouter#enable
Password:
MyRouter#show running-config
.
.
.
interface Ethernet1
 ip address 10.1.13.1 255.255.255.240
 ip access-group 100 in
 ip access-group 101 out
  .
  .
  .
```

Si la lista de acceso cuestionable está aplicada, revise dos veces que la lista de acceso se aplique en la dirección correcta para la interfaz. Si no se puede verificar por completo, desactívela temporalmente para ver si el tráfico puede pasar por el enrutador sin ella. Hay dos listas de acceso en nuestro ejemplo, de modo que les habilitaría ambas para ver si el problema está siendo causado por las listas de acceso. Para que se habilite a las listas de acceso en la interfaz hará lo siguiente:

```
MyRouter#config terminal
MyRouter(config)#interface ethernet1
MyRouter(config-if)#no ip access-group 100 in
MyRouter(config-if)#no ip access-group 101 out
```

En caso de que lo olvide, el modificador **in** en el extremo de cada instrucción del grupo de acceso configura las listas de acceso que habrán de aplicarse a los paquetes entrantes solamente. Un modificador **out** haría lo opuesto; la ausencia de un modificador aplica la lista al tráfico entrante y saliente.

Una vez que las listas de acceso estén deshabitadas, trate de establecer la conexión entre el host y el servidor que se reporta que no responde. Si el tráfico pasa con las listas de acceso deshabitadas, entonces una instrucción en algún lado de las listas de acceso probablemente sea la causa. El siguiente paso consiste en ver cuál lista contiene el problema al rehabilitar una de las dos. La lista de acceso 101, con todas sus reglas, es la más sospechosa. Para descubrir si éste es el caso, impóngala de regreso con el siguiente comando:

```
MyRouter(config-if)#ip access-group 101 out
```

Ahora trate nuevamente de conectarse al servidor. Si el problema ha regresado, ha establecido que el problema reside en algún lugar dentro de la lista de acceso 101.

Para depurar la lista de acceso, revísela cuidadosamente para encontrar la regla ofensora. Puede ser una regla de negación mal colocada, pero un puerto faltante TCP o UDP en una regla de permiso también podría ser el problema. No olvide revisar cualquier error de ortografía en su ACL. Una simple dirección IP mal escrita puede fácilmente ser la causa de su problema.

Recuerde que cada regla de lista de acceso debe declarar a cuál protocolo de transporte IP se aplica: TCP, UDP, ICMP. Sin embargo, con más frecuencia los puertos de la aplicación ofensores son el origen del problema, simplemente porque son muchos de ellos y las aplicaciones de red que se están usando cambian con frecuencia. Por ejemplo, si los usuarios están teniendo un problema al establecer una conexión a un servidor Web, revise para asegurarse de que el número de puerto HTTP 80 está permitido entre las direcciones de host y servidor.

También es posible que el tráfico se esté negando antes de llegar a una regla de permiso diseñada para dejarlo pasar. Recuerde que las listas de control de acceso se leen de arriba hacia abajo hasta que se encuentra una coincidencia. Si éste es el caso, la secuencia en que las reglas aparecen en la lista debe ajustarse de acuerdo con ello para colocar las reglas prioritarias cerca de la parte superior.

Redireccionamiento del tráfico desde áreas congestionadas En ocasiones el tráfico se vuelve congestionado en un enrutador determinado. Esto podría deberse a que nuevos hosts usan el agregado en el área, nuevas aplicaciones de red han salido a línea u otras causas. Cuando esto sucede, inicie sesión en el enrutador congestionado e ingrese el comando **show ip traffic** para generar el siguiente informe:

```
MyRouter#show ip traffic
IP statistics:
  Rcvd:  7596385 total, 477543 local destination
         0 format errors, 0 checksum errors, 96 bad hop count
         0 unknown protocol, 1 not a gateway
```

```
        0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 53238 received, 280 sent
  Mcast: 205899 received, 521886 sent
  Sent:  738759 generated, 6113405 forwarded
         13355 encapsulation failed, 374852 no route
.
.
.
```

Además de reportar el tráfico IP, el comando **show ip traffic** informa en el tráfico generado por los protocolos de transporte, los protocolos enrutamiento, las solicitudes de traducción ARP, incluso la manera de comprender las cargas que se han estado poniendo en el enrutador y cuáles opciones podría tener para aligerarlas.

Por ejemplo, si el tráfico de transmisión parece excesivo, tal vez podría tratar de endurecer las restricciones en las listas de acceso que rigen los enrutadores de alrededor. Pero, al parecer todo o casi todo el tráfico pesado es legítimo, el tráfico que afecta a los enrutadores vecinos también debe analizarse. Si hay una inequidad de las cargas entre los enrutadores de similar capacidad, tal vez lo que se necesite sea el equilibrio de carga. En casi todos los casos, esto tiene más sentido que comprar más hardware con más poder.

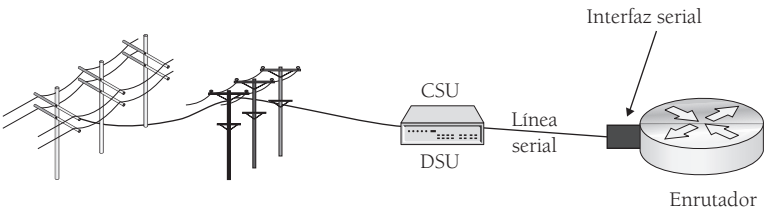
Una manera de equilibrar las cargas de tráfico entre los enrutadores consiste en iniciar sesión en el enrutador congestionado e ingresar en el modo config-router al llamar a los protocolos enrutamiento; luego establecer las mediciones de distancia para cada enrutador para dirigir el tráfico lejos del enrutador congestionado hacia un vecino menos congestionado.

Detección y solución de problemas de vínculos WAN

La detección y solución de problemas en WAN incluye el uso de un conjunto diferente de herramientas. Esto es porque casi todas las conexiones en los vínculos WAN deben atravesar una línea serial. Para recordar un poco sobre el tema, una línea serial conecta una unidad CSU/DSU a un enrutador. Las redes telefónicas no transmiten señales usando una tecnología de red de capa de vínculo de datos (capa 2) como Ethernet. Los enrutadores no son conmutadores telefónicos, de modo que las transiciones entre las dos tecnologías debe hacerse de alguna manera. La interfaz CSU/DSU a línea serial le da al enrutador señales que puede comprender.

NOTA Un CSU/DSU es como un módem, pero trabajan con líneas digitales en lugar de analógicas. CSU (Channel Service Unit, unidad de servicios de canal) es una interfaz que conecta a una línea telefónica digital, como T1 (en lugar de un modelo que conecta a una línea telefónica analógica). DSU (Data Service Unit, unidad de servicios de datos) es un dispositivo que se data al extremo del cliente de la conexión, por lo general en enrutador o un conmutador LAN.

Los vínculos seriales tienen una importancia obvia porque extienden las interconexiones más allá del campus de la oficina a ubicaciones remotas. Un vínculo remoto de cualquier tamaño requiere el uso de un circuito de teléfono digital de algún tipo, que va desde un T1 fraccional hasta una línea T3 completa (DS3).



Una línea serial proporciona una ventana a través de la cual todo el vínculo WAN puede diagnosticarse. En otras palabras, no sólo puede analizar la línea serial y sus interfaces sino admirar el tráfico que lleva, también puede diagnosticar el bucle telefónico digital y, en alguna medida, lo que está pasando en el extremo remoto del vínculo.

Diferencias en el informe de show interfaces serial

Cisco proporciona una herramienta especial para detectar y solucionar problemas de vínculos seriales en el comando **show interfaces serial**. Es muy parecido al comando **show interfaces** común, pero con algunas diferencias importantes, como se destaca en la figura 15-9. Específicamente, muestra información para el puerto serial.

Una manera en que los vínculos seriales se diferencian es el tipo de encapsulamiento usado en los bucles telefónicos digitales. El protocolo de encapsulamiento High-Level Data-Link Control (HDLC, control de vínculo de datos de alto nivel) es indicado en el cuadro sombreado de la parte superior de la figura 15-9. El encapsulamiento es necesario para mantener los paquetes de Ethernet en el vínculo telefónico digital. En ocasiones, el encapsulamiento pudo desactivarse inadvertidamente, de modo que el campo Encapsulation debe estar seleccionado.

Otra diferencia es que las conversaciones (sesiones) se informan en el informe **show interfaces serial** *número_interfaz*. Los vínculos WAN tienen menos ancho de banda que los medios compartidos locales. Un circuito T1 (DS1) tiene una velocidad de datos de 1.544 Mbps, y uno T3 (DS3) tiene una de 45 Mbps. Casi todas las empresas usan T1 o T3 fraccional al comprar canales dentro de ellas (T1 tiene 24 canales; T3 tiene 672). Por tanto, el ancho de banda WAN está limitado en comparación con, por decir algo, un segmento LAN de 100 Mbps, y en ocasiones una sesión de usuario determinada toma más de lo que comparte. Por tanto, cuando se detectan y solucionan problemas con un vínculo WAN, resulta de ayuda saber cuántas conversaciones están activas. En caso de que se lo pregunte, el campo Reserved Conversation se relaciona con el Resource Reservation Protocol (apodado RSVP, protocolo de reservación de recursos). RSVP es un estándar de la industria diseñado para usarse con herramientas de QoS (Quality of Service, calidad de servicios) para ayudar a garantizar los niveles de servicio.

El cuadro en la parte inferior de la figura muestra una tercera diferencia en el informe **show interfaces serial** *número_interfaz*. Esos cinco campos son los mismos que las luces para parientes que tal vez haya notado en los módems externos. Por ejemplo, DTR (Data Termi-

```
RemoteRouter>show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.14.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 217/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/390 (size/max/drops); Total output drops: 54920
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/12921 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 39000 bits/sec, 52 packets/sec
  5 minute output rate 36000 bits/sec, 48 packets/sec
     26405 packets input, 1977458 bytes, 0 no buffer
     Received 12385 broadcasts, 0 runts, 0 giants, 0 throttles
     1294 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 397 abort
     4783008 packets output, 2510565558 bytes, 0 underruns
     0 output errors, 0 collisions, 9172 interface resets
     0 output buffer failures, 0 output buffers swapped out
     12 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Figura 15-9. Casi todos los vínculos WAN todavía usan líneas seriales para conectar enrutadores a bucles telefónicos.

nal Ready, listo para terminar de datos), es un circuito EIA/TIA-232 (née RS-232) que se activa para notificar a los equipos de comunicación de datos en el otro extremo que el host estar listo para enviar y recibir datos. DCD (Data Center Detect, detección de portadoras de datos) es importante porque percibe la señal del portador real (el ruido del módem que escucha cuando hace la conexión con el módem). Los cinco circuitos de módem se incluyen en el informe **show interfaces serial** *número_interfaz* para detección y solución de problemas de vínculos seriales que se ejecutan sobre líneas análogas/módem de líneas digitales.

Campos de diagnóstico claves en el informe show interfaces serial

Los vínculos seriales difieren por naturaleza de los segmentos LAN, de modo que el diagnóstico, da un enfoque diferente. Ciertas cosas que, en cierta medida, se dan por sentadas en los vínculos de segmento LAN suelen ser la causa de problemas de rendimiento o incluso de fallas en los vínculos seriales. En la figura 15-10 se resaltan los elementos que las personas encargadas de la detección y solución de problemas buscan primero en una interfaz serial.

Como puede ver, la detección de problemas en los vínculos seriales hace énfasis en la búsqueda de errores y en la actividad de la línea. Esto es natural, dado que la parte media de un vínculo WAN (el circuito telefónico) es básicamente invisible al equipo de red.

El porcentaje de carga de la línea serial es alto, alrededor de 80%

```
RemoteRouter>show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.14.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 217/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/390 (size/max/drops); Total output drops: 54920
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/54920 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 39000 bits/sec, 52 packets/sec
  5 minute output rate 36000 bits/sec, 48 packets/sec
     26405 packets input, 1977458 bytes, 0 no buffer
     Received 12385 broadcasts, 0 runts, 0 giants, 0 throttles
     1294 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 397 abort
     4783008 packets output, 2510565558 bytes, 0 underruns
     0 output errors, 0 collisions, 9172 interface resets
     0 output buffer failures, 0 output buffers swapped out
     12 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Números elevados de caídas de salida y de establecimientos sugiere que la línea se está utilizando en exceso

El conteo de errores de entrada es relativamente bajo

Figura 15-10. Ciertos campos suelen ser el centro de atención cuando se detectan y solucionan problemas en un vínculo serial.

Al revisar la figura 15-10, vemos un caso en que el tráfico entrante parece estar bien, pero se están eliminando una gran cantidad de paquetes de salida. Dado que la línea serial se está utilizando mucho, ejecutándose casi el 80% del ancho de banda disponible, podemos concluir que los paquetes se eliminan a causa del uso excesivo, no a la falta de hardware en el vínculo.

La primera línea de salida en la figura 15-10 también puede ayudarle en los esfuerzos de detección y solución de problemas. En el despliegue **show interfaces serial**, la primera línea le dará una de las cinco indicaciones de estado. Lo ideal es que, como lo muestra la figura 15-10, usted quiera que en esta línea se lea "Serial *x* is up, line protocol is up". Sin embargo, si hay un problema, ese estado podría ser uno de los siguientes:

- **Serial *x* is down, line protocol is down**. Ésta es una indicación de que el enrutador no está recibiendo una señal de la conexión WAN, hay un problema con el cableado o incluso un problema en la compañía telefónica.
- **Serial *x* is up, line protocol is down.** Ésta es una indicación de que un enrutador local o remoto ha sido configurado mal, el enrutador remoto no está transmitiendo los mensajes keepalives, una unidad de servicio de canal local o remoto o las unidades de servicio digital han fallado.

- **Serial *x* is up, line protocol is up (looped).** Ésta es una indicación de que hay un bucle en el circuito.
- **Serial *x* is up, line protocol is down (disabled).** Ésta es una indicación de que hay una tasa elevada de errores debido a un problema con el portador telefónico, la unidad de servicio de canal 11 o las unidades de servicios digitales están experimentando un problema, o la interfaz del enrutador está fallando.
- ▲ **Serial *x* is administratively down, line protocol is down**. Ésta es una indicación de que la configuración del enrutador incluye el comando **shutdown** o que existe una dirección IP duplicada.

Detección y solución de problemas de errores de entrada en la línea serial Una de las causas más comunes de problemas en la línea serial son los errores de entrada (en otras palabras, los datos entrantes del sitio remoto). Las causas probables de los errores de entrada de línea serial, con las acciones sugeridas, se delinean en la tabla 15-5.

Detección y solución de problemas de errores de entrada y salida en la línea serial Otra pista para problemas en la línea serial es un incremento en los paquetes eliminados en la interfaz. Un paquete se *elimina* cuando demasiados paquetes se están procesando en el sistema y no hay memoria de búfer insuficiente para manejar los paquetes. Eso se aplica tanto a las eliminaciones de entrada como de salida, como se delinea en la tabla 15-6.

Síntomas de los errores de entrada	Causas probables y acciones sugeridas
Errores de entrada junto con errores de CRC o de marco	Una línea sucia, donde el ruido eléctrico interfiere con la señal de datos. El cable serial excede la longitud máxima especificada para el tipo de circuito telefónico. El cable serial no está protegido. El circuito telefónico puede estar funcionando mál. **Acciones:** Reduzca la longitud del cable. Instale cables protegidos. Revise el bucle telefónico con un analizador de línea. La medición del tiempo oscila en la línea donde las señales de datos varían de las posiciones de tiempo de referencia, o aparece sesgada donde los relojes del dispositivo están establecidos de manera diferente. **Acciones:** Asegúrese de que todos los dispositivos estén configurados para usar un reloj de línea común.
Errores de entrada junto con abortos	La transferencia de un paquete eliminado en una transmisión a medias. Por lo general causada por un restablecimiento de la interfaz en el enrutador que se está analizando. También puede ser causada por un restablecimiento del enrutador remoto, un mal circuito telefónico o una mala CSU/DSU. **Acción:** Revise el hardware local, luego el hardware remoto. Reemplace el equipo con falla.

Tabla 15-5. Causas y acciones en los errores de entrada.

Síntomas de la eliminación de paquetes	Causas probables y acciones sugeridas
Aumento en la cantidad de paquetes de entrada eliminados	Las eliminaciones de paquete en la entrada suelen ocurrir cuando el tráfico se está encontrando desde la interfaz local (Ethernet, Token Ring, FDDI) que es más rápida que la interfaz serial. El problema suele surgir durante los periodos de tráfico elevado. **Acciones:** Aumento en el tamaño de la cola que mantiene la entrada de la interfaz en el archivo config del enrutador.
Aumento en la cantidad de paquetes de salida eliminados	Las eliminaciones de paquetes de salida suelen ocurrir cuando no hay disponible búfer de sistema en el momento en que el enrutador está tratando de entregar el paquete al búfer de trasmisión durante etapas de tráfico elevado. **Acciones:** Aumento en el tamaño de la cola que mantiene la salida de la interfaz. Desactivación de la conmutación rápida. Implementación de la cola de prioridad.

Tabla 15-6. Causas de paquetes eliminados y acciones que deben emprenderse.

Cuando las eliminaciones tienen lugar en una dirección pero no en la otra (entrada en comparación con salida) la persona que realiza la detección y solución de problemas puede señalar al origen del problema. Si ha sucediendo en ambas vías, el enrutador o su interfaz serial es probablemente culpable.

Detección y solución de problemas de vínculos seriales Casi todos nosotros hemos usado módems el tiempo suficiente para saber que en ocasiones con la conexión establecida puede fallar o incluso romperse. Esto también es válido para las líneas seriales, por lo general debido a restablecimiento de la interfaz o transiciones del portador, como se delinea en la tabla 15-7.

Aunque no haya segmentos LAN en sí, los vínculos seriales están integrados a interconexiones distribuidas geográficamente. No olvide tomarlos en cuenta, aunque un problema de línea serial no sea evidente al principio. Por ejemplo, cuando evalúe problemas de rendimiento, podría ser que un vínculo serial con falla esté desplazando las cargas de tráfico hacia algún otro lugar dentro de la interconexión.

VPN cliente-servidor

Como ya lo analizamos, las VPN son una manera costeable de usar Internet como su propia WAN privada. Se está teniendo problemas para hacer que una VPN funcione, hay cuatro áreas en las cuales suelen surgir los problemas con VPN:

- ▼ Tráfico de VPN bloqueado.
- ■ Malas conexiones de Internet.
- ■ Errores de configuración.
- ▲ Problemas de entunelamiento Network Address Translation (NAT, traducción de direcciones de red).

Síntomas de errores en línea	Causas probables y acciones sugeridas
Aumento en las transiciones de portador	Interrupción en la señal del portador. Por lo general debido al restablecimiento de la interfaz en el extremo remoto del vínculo. Los establecimientos pueden ser causados por orígenes externos como tormentas eléctricas, alertas de sobreuso de T1 o T3, o hardware con falla. **Acciones:** Use un cuadro de interrupción de señal o un analizador de seriales para revisar el hardware en ambos extremos. Luego revise el hardware del enrutador. Reemplace el hardware que esté fallando, de acuerdo con lo necesario. No es requerida ninguna acción si el problema se debe a una causa externa.
Incremento en los restablecimientos de interfaz	Los restablecimiento de interfaz se deben a mensajes Keepalive faltantes. Por lo general son resultado de transiciones de portador, falta de búfer, o un problema con hardware de CSU/DSU. La coincidencia con transiciones aumentadas de portador o errores de entrada indican un mal vínculo o un mal hardware CSU/DSU. **Acciones:** Use un cuadro de interrupción de señal o un analizador de seriales para realizar el hardware en ambos extremos. Contacte al comercializador de línea arrendadas si el hardware está funcionando bien.

Tabla 15-7. Causas de errores de línea serial y acciones que hay que emprender.

A riesgo de insultar la inteligencia de alguien, cuando surgen los problemas (no sólo problemas de VPN), lo primero que hay que hacer es revisar los cables sueltos. Revise los cables en el módem del cliente, el enrutador y el firewall para asegurarse de que están conectados apropiadamente. También es una buena idea asegurarse de que esté usando cableado correcto Cat 6 o 7 y que no eligió cable cruzado.

Tráfico de cuello de botella

El siguiente paso consiste en asegurar que su Internet Service Provider (ISP, proveedor de servicios de Internet) permite tráfico IPSec, VPN. Si no lo hace, no importa que su VPN esté configurada apropiadamente, porque los paquetes no van a ningún lado. Si su ISP no permite tráfico IPSec VPN, tal vez debe considerar el cambio a otro ISP.

Revise su firewall para asegurar que no esté bloqueando el tráfico IPSec o PPTP. Para establecer una conexión VPN, es necesario configurar el tráfico IPSec saliente en el firewall. Para ello, debe configurar su firewall para habilitar IPSec, y después crear una regla que permita el pasaje del tráfico entre la LAN y WAN. Si no es posible, tal vez sea necesario localizar el cliente en el DMZ o considerar la inversión en un enrutador o un firewall diferente.

No sólo los firewalls de hardware pueden bloquear el tráfico sino que también lo pueden hacer los de software. Esto es otro lugar fácil de revisar, sobre todo en el caso de clientes que están viajando o tratando de conectarse desde ubicaciones que no están equipadas con firewalls de hardware, sino que están configuradas con firewalls de software. Sólo deshabilite el firewall de software y vea si eso funciona. Algunos firewalls de software le preguntarán si debe permitir que el tráfico VPN pase y puede agregar la dirección IP de destino deseada a la configuración de la zona confiable.

NAT

Asegúrese de que su NAT está entunelada correctamente. Un buen lugar para empezar es asegurarse que tiene casi todas las actualizaciones de firmware de software. Cuando IPSec trata de verificar la integridad de los paquetes, NAT cambia la dirección IP de origen a la dirección WAN del firewall para navegar apropiadamente por Internet. Por desgracia, esto causa problemas con IPSec porque los paquetes fallan en la revisión de integridad.

Puede obtener un listado de sus traducciones de NAT y una revisión general de sus estadísticas de NAT empleando dos comandos EXEC simples:

- ▼ **show ip nat translation verbose** Esto despliega la actividad de traducciones de NAT con información adicional para cada tabla de traducción, incluido el tiempo que se ha acusado a la entrada.
- ▲ **show ip nat statistics** Esto despliega varias estadísticas de NAT, incluido el número de traducciones activas, las interfaces y las traducciones totales.

Configuración

La configuración también puede ser culpable cuando se trata de rastrear los problemas de VPN. Asegúrese de que las direcciones IP correctas se estén usando. En el caso de las VPN clientes, la revisión y renovación de las direcciones IP en Windows se realiza al abrir un indicador de comandos y luego ingresar **ipconfig/all**.

Si la dirección IP emitida por el administrador de red para conectarse a la VPN no cae dentro del rango mostrado, entonces la dirección IP no es válida. Para corregir esto, renueve el arrendamiento. Esto se logra al abrir una ventana de indicador de comandos y escribir **ipconfig/renew** y la dirección IP del adaptador.

NOTA Si el cliente está usando PPPoE para conectarse al ISP (lo que será el caso si no se ha asignado una dirección IP estática) asegúrese de que el cliente esté conectándose a Internet utilizando cualquier aplicación de conexión que sea necesaria.

Envíe un comando **ping** a la dirección IP del su servidor VPN. Si obtiene una respuesta, entonces sabe que el cliente está conectado a Internet y puede ver el servidor VPN. A continuación, debe descartar cualquier problema de configuración de DNS. Esta vez, realice una prueba de ping, pero use nombres de dominio (por ejemplo, www.velte.com). Si tiene una respuesta, la conexión a Internet está funcionando bien. De lo contrario, significa que DNS está mal configurado en el cliente o en del propio servidor DNS.

El cliente y el servidor VPN deben tener la capacidad de hablar el mismo lenguaje para hacer el trabajo. De esta manera, es importante asegurarse que las configuraciones de cifrado en el cliente y en el servidor VPN sean las mismas. Los algoritmos de autentificación deben

estar configurados apropiadamente en el cliente y en el servidor VPN. Ambos dispositivos necesitarán el secreto compartido o, si son certificados, la clave pública correcta, si es necesario.

Malas conexiones

A continuación, revise si el cliente está tratando de conectarse en una conexión lenta. La latencia puede causar fallas en las conexiones VPN, porque les gusta el tráfico consistente; de otra manera, tienden a fallar. Lo más probable es que vea esto como un problema con las conexiones satélite donde la latencia puede ir de medio segundo a varios segundos.

La velocidad de conexión puede revisarse con la herramienta ping. Usando el interruptor "-t", puede obtener una prueba continua de velocidades de conexión entre el cliente y el servidor VPN. Por ejemplo:

```
ping 68.93.44.123 –t
```

Esto produce una lista de los esfuerzos de la prueba por enviar paquetes a la dirección. La prueba se termina al oprimir CTRL+C. Eche un vistazo a los resultados. Si ve cualquier mensaje de error "Request timed out", trate de aumentar el valor de tiempo de espera para que pueda medir de manera exacta cuánta latencia sufre su conexión. Este valor puede cambiarse al usar el interruptor "-w". Por ejemplo:

```
ping 68.93.44.123 –t-w 7000
```

Esto aumenta el valor de tiempo de espera a 7 000 ms. Esto debe ser suficiente para indicar cuánta latencia está presente en su vínculo. Tiempos de conexión de 1 500 ms y superiores causarán que el vínculo VPN falle.

NOTA Tal vez no suene importante a primera vista, pero si el servidor VPN y el cliente no están en las zonas horarias correctas y tienen la configuración correcta de tiempo, tal vez no sean capaces de conectarse. Esto se debe a que la configuración de tiempo correcta es necesaria para la expiración de la clave.

DETECCIÓN Y SOLUCIÓN DE PROBLEMAS DEL HARDWARE DE CISCO

Cuando la ubicación probable del problema se ha identificado, el primer paso es examinar físicamente y probar el dispositivo sospechoso. Esto identificará la causa del problema en un número sorprendente de situaciones de detección y solución de problemas. En ocasiones, el problema es causado por algo tan simple como un componente suelto; otras veces, algo está dañado.

Inspección de los dispositivos

Una vez que se ha identificado un dispositivo sospechoso, debe inspeccionarlo físicamente. Esto es un procedimiento de rutina. (Aunque un dispositivo sospechoso con problemas esté en una ubicación remota, se envía una persona de contacto para hacer una inspección.) Al principio, establecimos que casi todas las tareas de detección y solución de problemas se ha-

cen desde el escritorio del administrador, y eso es verdad. Casi todas las tareas se hacen desde la PC del administrador o desde una consola NMS. Sin embargo, no hay un sustituto para la revisión real de un dispositivo para ver lo que está pasando. Las dos partes de la inspección de un dispositivo son la lectura de sus LED y de inspección de los componentes del dispositivo.

Lectura de los LED del dispositivo

Si el dispositivo está en línea, lo primero que hay que hacer es leer los LED (Light-Emitting Diodes, diodos emisores de luz). Tal vez reconozca los LED como las luces brillantes en la parte frontal de muchos dispositivos electrónicos. Casi todos los dispositivos de red tienen LED como ayuda para la detección y solución de problemas. La organización del banco de LED sigue el diseño del dispositivo:

- ▼ **Dispositivos de acceso con un banco de puertos en la parte frontal, con una conexión de cable del atentado en cada puerto utilizando un colector estilo telefónico RJ-45**. Los productos desde el conmutador cisco Catalyst 2800 hasta el Catalyst 4500 satisfacen esta descripción. Por lo general hay un LED por puerto.
- ■ **Enrutadores basados en tarjetas madre con segmentos LAN conectados en la parte trasera, por lo general mediante cables de par trenzado, pero también cables de fibra óptica para uplinks**. El enrutador cisco 7200 satisface esta descripción. Los LED en estos dispositivos aparecen detrás de los paneles de plástico ahumado en la parte frontal de las cajas.
- ▲ **Enrutadores y conmutadores de alto desempeño de la configuración bus y cuchilla, una vez más con conectores de red en la parte trasera, tanto de fibra óptica como de cable de par trenzado**. El enrutador cisco 7500 y el conmutador Catalyst 6500 satisfacen esta descripción. Los LED en estos dispositivos aparecen detrás de los paneles de plástico, no en la parte frontal y en las cuchillas (módulos de tarjetas) en la parte trasera (recuerde que una cuchilla es básicamente un enrutador o un conmutador completo en una tarjeta).

A los LED también se les denomina *luces de actividad*. Cada LED en un dispositivo de acceso representa un host. Los LED de enrutadores y conmutadores LAN representan segmentos LAN completos.

Los LED parpadean y cambian de color de acuerdo con el estatus del puerto. Verde significa correcto, y naranja significa que el puerto está empezando a funcionar. Si el puerto no funciona, su LED se oscurece. El LED del puerto parpadea con los paquetes que están pasando a través de él. Una práctica común es presionar Reset para ver lo que sucede. Temporalmente, los LED se vuelven anaranjados o incluso rojos si encuentran problemas durante el ciclo de alimentación eléctrica. Con el tiempo, pasarán a verde, pero la condición de error temporal puede indicar un error de configuración no fatal.

La regla es que si una luz de actividad está verde, la línea está bien. Si la luz es anaranjada, la línea está operando pero funcionando mal. Si la luz de actividad está apagada, la línea no funciona.

Inspección física de los dispositivos

El siguiente paso es inspeccionar físicamente el propio dispositivo. Empiece por asegurarse de que el dispositivo esté fuera de línea, y luego quite la cubierta de la parte superior del gabinete del dispositivo e inspeccione el interior, mirando de la manera siguiente:

- ▼ **Conexiones sueltas** Busque cualquier tarjeta (módulo) o cable que parezca suelto. Vuelva a colocar cualquiera que se encuentre.
- ■ **Nuevas tarjetas** Si sabe que alguna tarjeta es nueva, vuelva a colocarla en su conexión varias veces. Las tarjetas nuevas son más propensas a la oxidación al cubrirse con una capa de carbón en las conexiones de su plano trasero.
- ■ **Partes quemadas o dañadas** Busque cualquier cable, cinta de conexión o tarjeta quemada. También busque en el plano trasero para ver si todo está bien. Inspeccione de cerca los cables que van a la fuente de poder del dispositivo, también busque cualquier cable doblado.
- ▲ **Interior del dispositivo sucio** Si el dispositivo tiene polvo y grasa en el interior, apáguelo y límpielo. Los dispositivos pueden acumular una gran cantidad de sustancias extrañas del aire en entornos polvosos o sucios, lo que a veces puede afectar el desempeño.

Después de completar la inspección, trate de reiniciar el dispositivo para ver si el ciclo de alimentación eléctrica corregirá el problema. Y una precaución importante: no cambie nada en la configuración. Al hacerlo antes de reiniciar puede dificultar la determinación del origen del problema después de eso. Sólo agrega más variables a la mezcla.

La prueba de reinicio

Si no se encontró ningún problema grave durante la inspección del dispositivo, el siguiente paso consiste en probar el ciclo de alimentación eléctrica para ver cómo responde. El ciclo de alimentación eléctrica consiste en apagar el dispositivo y luego encenderlo de nuevo, lo que probablemente sepa qué es la cura para cualquier problema en Microsoft Windows. Como vimos en el capítulo 3, el reinicio de los dispositivos puede indicar mucho acerca del estado de éste, y en algunos casos, incluso puede hacer que el problema desaparezca.

Cuando reinicia, si la configuración en memoria no coincide con el hardware, pueden surgir diversos problemas. Es probable que los puertos dejen de funcionar, que ocurran errores de tiempo de espera en el bus, etcétera. Si el dispositivo se reinicia y le pide una contraseña, la circuitería y la memoria están trabajando adecuadamente. Algunos síntomas importantes y probables causas se delinean en la tabla 15-8.

Cuando se encuentran problemas de hardware en este extremo, es hora de llamar al soporte de Cisco o una organización de mantenimiento independiente con la que su empresa tenga un contrato. Por lo general, los dispositivos envían al centro de mantenimiento para reparación en su taller. Sólo las empresas y usuarios finales con partes sobrantes, personal entrenado por Cisco e instrumentos apropiados tratan de reparar los dispositivos de hardware de red en casa.

DETECCIÓN Y SOLUCIÓN DE PROBLEMAS DE CONFIGURACIONES DE RED

A medida que su red crece y evoluciona, probablemente encontrará algunos segmentos LAN que tienen capacidades inalámbricas (y su propio conjunto de problemas). Además, lo más probable es que quiera dar seguimiento a temas relacionados con el rendimiento gene-

Síntoma de reinicio	Causas probables
No hay respuesta	Mal suministro de fuente eléctrica; fusible quemado; interruptor de encendido en mal estado; conector en mal estado; plano trasero en mal estado.
No se reinicia	Suministro de energía eléctrica deficiente o mal conectado; tarjeta de procesador en mal estado (o mal insertada); tarjeta de memoria en mal estado; imagen IOS dañada en NVRAM; cables cortados.
Reinicio parcial o constante	Procesador, controlador o tarjeta de interfaz en mal estado; plano trasero dañado; suministro de energía eléctrica deficiente; mal microcódigo.
No se muestran las tarjetas en el despliegue de inicio	Procesador, controlador o tarjeta de interfaz en mal estado; plano trasero dañado; tarjetas no insertadas en el plano trasero; suministro de energía eléctrica deficiente.

Tabla 15-8. Problemas típicos de reinicio y causas probables.

ral de su red. En esta sección, echaremos un vistazo de cerca a algunos buenos métodos para localizar y corregir problemas que surgen de los temas de rendimiento.

Redes inalámbricas

Las redes inalámbricas proporcionan un nuevo nivel completo de conveniencia al mundo de las redes. La capacidad de conectar computadoras sin tener que preocuparse acerca del cableado (sin mencionar la capacidad de llevar su laptop a cualquier lugar de la oficina) y aún mantener la conectividad de red es un enorme punto adicional.

Muchos despliegues inalámbricos empiezan a funcionar en cuanto se conecta su punto de acceso y su tarjeta inalámbrica. Por ejemplo, si está usando una versión Plug-and-Play de Windows (como Windows XP, por ejemplo), casi siempre la tarjeta inalámbrica se reconocerá instantáneamente y, temas de seguridad aparte, tendrá acceso a la red sin problemas. Lo malo es que no siempre funciona con esta simplicidad.

Filtro de direcciones

Al igual que muchas facetas en las redes, lo que se hace para mantener a los chicos malos fuera también puede mantener a los chicos buenos fuera. Uno de los métodos de seguridad de WiFi es el filtro de direcciones MAC e IP. Es decir, su AP (Access Point, punto de acceso) puede configurarse para permitir o rechazar el tráfico de direcciones IP o MAC específicas. Si un cliente o varios clientes tienen problemas para conectarse, asegúrese de que sus direcciones IP o MAC no están siendo bloqueadas por el AP. Cuando se configura apropiadamente, sin embargo, esta característica es una excelente manera de agregar una capa de seguridad.

Interferencia de canal

En una red 802.11b/g, en realidad sólo hay tres canales útiles: los canales 1, 6 y 11. Si está teniendo problemas con su red, podría revisar si no hay otras redes existentes en uno de sus canales. Tal vez esté experimentando interferencia de otro dispositivo en su propia red, o tal vez experimente complicaciones debido a la red inalámbrica del vecino. La solución a su problema podría ser tan simple como cambiar el AP y el canal de los clientes.

Cifrado

El medio ideal de puridad para su red inalámbrica es emplear la autentificación 802.1x junto con cifrado. Sin embargo, si no está utilizando autentificación, por lo menos debe usar cifrado. Un componente que suele ser pasado por alto en las redes inalámbricas es la habilitación de cifrado en sus puntos de acceso y sus clientes. Como se mencionó en el capítulo 8, esto es extremadamente importante para la protección de sus datos.

Si no se habilita el cifrado, es relativamente fácil que alguien husmee el tráfico de red inalámbrico y recoja todo tipo de información, desde el ID de usuario y la información de contraseña hasta el contenido de correos electrónicos que se están enviando y recibiendo.

Aunque se ha encontrado que es muy inseguro, Wireless Equivalent Privacy (WEP, privacidad equivalente inalámbrico) es aún el protocolo de cifrado más común en uso hoy en día. Utiliza una clave que éste establece en el punto de acceso y los ingresa en sus dispositivos inalámbricos. Esta clave se usa para cifrar los datos que se están transmitiendo y descifrar los datos entrantes. Sin la clave, nadie más puede "ver" los datos que se están transmitiendo.

El siguiente nivel de seguridad inalámbrica es el WiFi Protected Access (WPA, acceso protegido WiFi). Es como WEP, pero proporciona un nivel mucho más elevado de cifrado y seguridad de autentificación. No está disponible en puntos de acceso antiguos, y puede requerir una actualización en el lado del cliente para habilitarlo allí. Si no puede usar WPA, por lo menos ejecute WPE (algún cifrado, aunque se ha llegado a descifrar mensajes completos en WEP) es mejor que nada.

NOTA Es aconsejable familiarizarse con el cifrado y las características generales de seguridad disponibles en su hardware y su software (los estándares y las tecnologías avanzan rápidamente en la arena inalámbrica, y en ocasiones, un entorno más seguro está sólo a una actualización de firmware o software de distancia.

WEP Sin embargo, con el cifrado se incluyen una serie de problemas. Si su esquema descifrado es incorrecto en el punto de acceso o en los clientes, entonces deben esperarse problemas.

Si está experimentando problemas para hacer que sus clientes se conecten, el primer lugar para empezar es revisar la configuración de cifrado. Sigua estos pasos para asegurarse de que sus parámetros de cifrado sean correctos:

1. **Deshabilite el cifrado** Aunque acabamos de decir que es importante tener habilitado el cifrado, si lo deshabilita y aún está teniendo problemas, entonces el cifrado no tiene la culpa. Si resulta que todo se está ejecutando bien, vaya al paso 2.
2. **Conteo de caracteres** Revise su punto de acceso y las instrucciones de su tarjeta WiFi para asegurarse que está ingresando el número correcto de caracteres para la clave de cifrado. Por ejemplo, cuando usa una clave WEP de 40 bits, Cisco Airo-

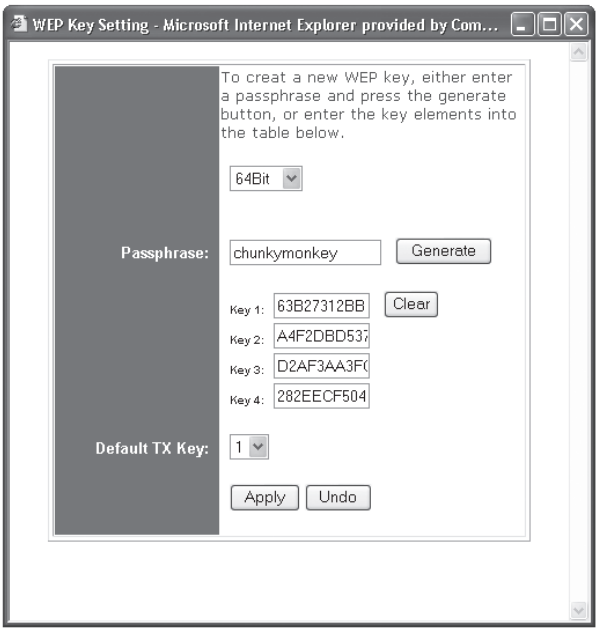


Figura 15-11. Una equivocación al escribir un carácter en WEP puede hacer que fallen las redes WiFi.

net 350 requiere de cinco caracteres ASCII a 10 extras decimales para su clave de cifrado (esto se muestra en la figura 15-11). También revise si debe especificar que está usando una cadena ASCII o una hexadecimal para la clase. En la tabla 15-9 se muestra cuántos caracteres se necesitan para varias longitudes de bits de claves.

3. **Configure los métodos de autentificación**. Cuando usa WiFi, hay dos tipos de autenticación: *sistema abierto* y *clave compartida*. Configure el punto de acceso y el cliente para permitir sistemas abiertos con lo que deshabilita WEP. Cuando habilite WEP de nuevo, cambie la autentificación de clave compartida. Esto proporciona una seguridad óptima.

Niveles de bit de WEP	ASCII	Hexadecimal
40/64	5 caracteres	10 caracteres
128	13 caracteres	26 caracteres

Tabla 15-9. El número de carácter es necesario en varias longitudes de clave.

4. **Haga que coincidan sus niveles de WEP** Aunque es posible mezclar entornos en que estén operando dispositivos de 40/64 y 128 bits (hablaremos acerca de ello más adelante), es mejor asegurarse de que todos estén usando el mismo nivel. Es decir, si resulta que necesita trabajar en un entorno mezclado, los dispositivos de 128 bits pueden hablar con dispositivos WEP de 40/64 bits, pero sólo si se configuran para usar las claves de 40 bits.
5. **Revise sus frases clave** Algunos comercializadores de WiFi (incluido Cisco) le permite ingresar frases clave para la generación de claves. Es decir, no debe determinar con una cadena de caracteres hexadecimales. Si lo desea, puede incluir una frase simple. (Por ejemplo, en la figura 15-12 se muestra la frase clave "chunkymonkey" convertida en una clave WEP hexadecimal.) Se trata de una herramienta conveniente, porque cuando configura la clave, no necesitar cortar una serie de letras y números sin significado (es más fácil recordar "chunkymonkey" que "63B27312BB"). Cuando usa frases clave, hay un par de cosas que debe tener en mente. En primer lugar, mantenga corta la cadena de la frase. No es necesario que de frases como "supercalifragilisticoespialidoso" (no dará como resultado una clave que sea más segura que cualquier otra generada con una frase más corta). En segundo lugar, use letras y números solamente (no utilice espacios, signos de puntuación ni otros símbolos en la mezcla).

WPA Si está usando WPA o WPA2, hay un gran número de pequeños pasos en la configuración que podrían llevarlo a que se haga mal.

Mire otra vez la configuración WPA que delineamos en el capítulo 8. He aquí algunos orígenes de problemas que podrían ser posibilidades:

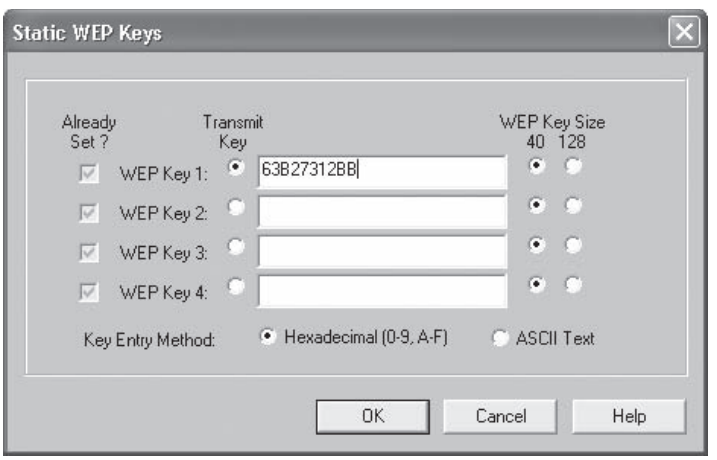


Figura 15-12. Pueden usarse frases clave para generar claves de WEP.

- ▼ Con WPA, la opción **Cipher** debe estar seleccionada y elegirse **TKIP** del menú desplegable.
- ■ WPA requiere que la clave de cifrado se introduzca en el número clave 2, no en el número clave 1. Asegúrese de que se ha establecido correctamente.
- ■ También debe seleccionarse el SSID correcto. Este valor se obtiene utilizando el SSID Manager y luego seleccionando el SSID del Current SSDI List.
- ▲ Tal vez también esté experimentando problemas dependiendo del método de autentificación que haya elegido (o que necesite elegir). El método de autentificación, que también es un conjunto de la pantalla SSID Manager, debe estar basado en el tipo de clientes que está usando su red WiFi. Si sólo tiene clientes de Cisco, seleccione Network-EAP. Si está usando clientes de terceros, seleccione Open Authentication with EAP. Si se encuentra en un entorno mezclado con clientes de Cisco y de terceros, seleccione Network-EAP y Open Authentication with EAP.

Además, eche un vistazo a las sugerencias para WEP. Como WPA y WPA2 utilizan claves, revise cosas como la longitud de las claves y asegúrese de que las claves se han ingresado apropiadamente en el AP y en los clientes.

Colocación de la antena e interferencia

Con una red inalámbrica, no necesita preocuparse demasiado por la interferencia de otros dispositivos. Por ejemplo, ejecutar la fotocopiadora probablemente no causará ningún problema con sus estaciones de trabajo inalámbricas, pero curiosamente puede hacer que su conexión inalámbrica deje de funcionar. Y aunque su laptop inalámbrica le permita la libertad de ir a cualquier lado de su oficina, sólo puede estar a una distancia de 30 a 100 m de su punto de acceso. Después de eso, la interferencia de las paredes, los pisos y otras obstrucciones causarán que las conexiones se vuelvan apreciablemente lentas o dejen de funcionar por completo. Por supuesto, esto aún es mejor que utilizar una conexión alámbrica, que sólo le permite ir hasta donde su cable Cat 5 se lo permita, lo que podría significar no ir más allá del extremo de su escritorio. La red inalámbrica puede valer la pena, sólo recuerde tener en mente dónde estarán sus dispositivos inalámbricos en relación con un punto de acceso. En casi todos los casos, pruebe y localice sus puntos de acceso de la manera más centralmente posible para sus clientes.

No importa dónde coloque sus puntos de acceso, siempre esté consciente de los orígenes de interferencia. Se mencionó antes que se sabe que las copiadoras reducen la conectividad en redes WiFi, pero también esté consciente de otros dispositivos que pueden causar estragos en su sistema. Un culpable importante viene con el disfraz de un teléfono inalámbrico de 2.4 GHz. Como opera en la misma frecuencia que 802.11b/g puede causar algunos dolores de cabeza. Si sospecha que un teléfono inalámbrico u otro dispositivo de 2.4 GHz, pruebe a usar otros canales WiFi para ver si las cosas mejoran.

Extensión del rango de su red inalámbrica ¿Qué pasa si no puede obtener una buena señal en algunas áreas de su espacio y realmente quiere que sean inalámbricos ahí? Después de descartar la interferencia de otros dispositivos, volver a colocar su antena, y tal vez reubicar sus puntos de acceso, tal vez quiera comprar un punto de acceso adicional. Este punto de acceso puede usarse para extender el rango de su red inalámbrica como se muestra en la figura 15-13.

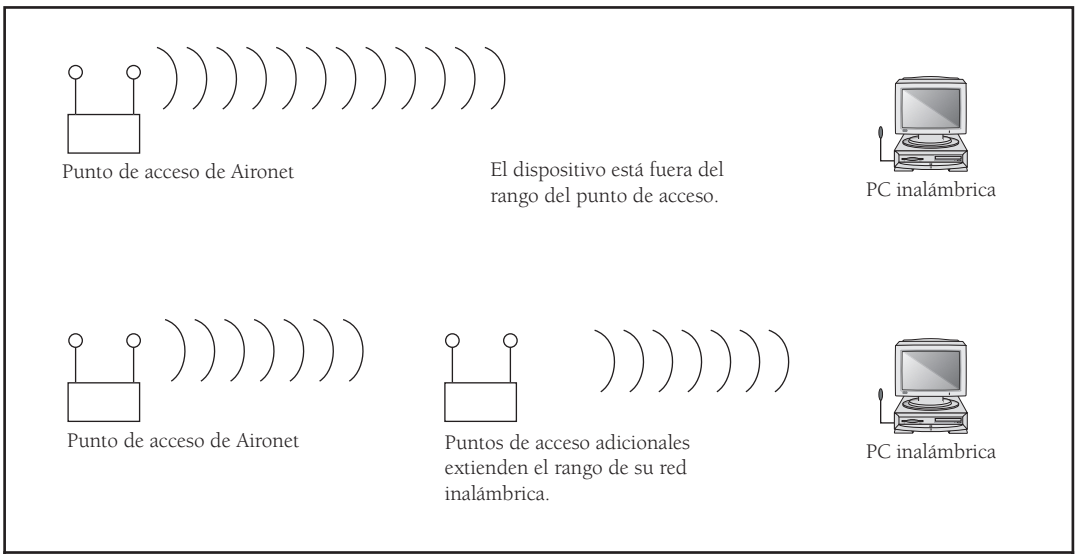


Figura 15-13. Es posible extender el rango de su red inalámbrica con puntos de acceso adicionales.

Cuando usa un punto de acceso para extender el rango, puede hacerlo sin necesidad de una conexión alámbrica al configurar el punto de acceso como puente desde un punto de acceso existente. Sólo asegure de que está monitoreando el rendimiento y la capacidad mientras crece la cuenta de usuarios, porque los puntos de acceso alámbricos pueden saturarse con el tráfico de la red y volverse un verdadero cuello de botella.

Revisión de sus niveles Una manera simple de revisar sus niveles de conectividad consiste en iniciar el cliente en el mismo cuarto o ubicación que el punto de acceso. Cuando logre que los dos dispositivos se comuniquen, es muy fácil empezar a mover el cliente lejos del punto de acceso. Esto le dará una idea rápida del rango entre los dos.

Sin embargo, puede explotar la conectividad de sus dispositivos con un poco más de finura al utilizar la Cisco Aironet Client Utility. Una vez iniciada en su cliente, esta aplicación, que se muestra en la figura 15-14, presenta la calidad y la fortaleza de la señal inalámbrica.

Detección y solución de problemas de punto a punto Si su vínculo de puente inalámbrico deja de funcionar, es posible que haya un problema con la antena en el cableado o los conectores de su sistema. Revise sus antenas y asegúrese que no estén fuera de alineación.

Además, las antenas y las conexiones pueden dañarse con la humedad. Si las antenas no están selladas apropiadamente cuando se instalan, la humedad puede condensarse dentro de los polos de alimentación de la antena, llenándose por completo con agua. La humedad que se abre paso en el cable coaxial puede ser incluso más problemática. Los cables coaxiales tienen un pie eléctrico interno de hule espuma. Esto puede actuar como una esponja, que envía humedad a todo lo largo del cable.

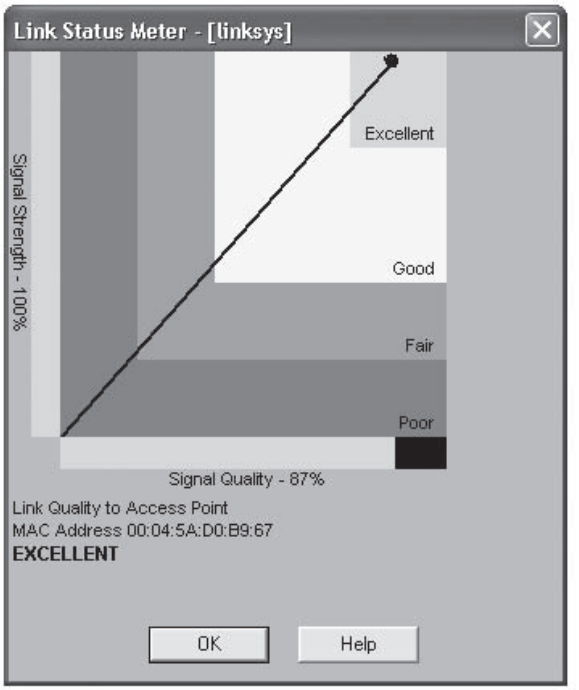


Figura 15-14. La Cisco Aironet Client Utility demuestra la fuerza y la calidad de su señal.

NOTA Si determina que el cableado coaxial está comprometido y está absorbiendo humedad, reemplace todo el cable, en lugar de remplazar unos cuantos metros y colocarle un nuevo conector.

Cuando los problemas se manifiestan en los sistemas en exteriores, el efecto aparecerá en ambos extremos del vínculo al mismo grado. Esto es relevante saberlo, porque si ve una señal degradada en un extremo de su vínculo, no piense automáticamente que ha encontrado la ubicación del problema. Muy bien podría encontrarse en el otro lado del vínculo. Revise ambos extremos.

Por otra parte, si la señal que recibe es baja en un extremo pero no en el otro, por lo general éste es un problema causado por una mala configuración de las unidades de radio o por interferencia. Como tales, no haga que una mala situación empeore al realinear las antenas. Si determina que la configuración es correcta y el equipo está trabajando apropiadamente, revise cualquier cosa que pudiera causar interferencia antes de ajustar las antenas.

Si sospecha que la interferencia es la culpable, examine su sistema y su comportamiento. ¿El problema es continuo o intermitente? Con más frecuencia, la interferencia ocurre de manera intermitente, cuando el origen de interferencia se activa.

En el caso de las redes inalámbricas de punto a punto, la determinación del origen de la interferencia puede ser una tarea horrenda. En primer lugar revise las antenas en cada extremo de su vínculo, ¿hay alguna otra antena presente? De ser así, haga un poco de investigación para determinar de quién son, quién las opera, en qué frecuencia opera, cuánto poder está transmitiendo y qué tipo de polarización de antena está usando.

Una vez que haya obtenido estos datos (podría ser tan simple como preguntar por el edificio en que está montada la antena), el siguiente paso consiste en preguntar al propietario si le gustaría ayudarle a determinar si su sistema es la fuente de la interferencia del suyo.

Cuando tenga toda la información pertinente acerca de la fuente de interferencia, puede resolver el problema mucho más fácil. En primer lugar, considere sus propias antenas. ¿Alguna de ellas estaba apuntando a las otras antenas del sistema? ¿Es posible reubicar sus antenas para que queden fuera de la ruta de transmisión del otro sistema?

A menudo, el cambio de la polarización de sus antenas a la polarización opuesta del sistema de interferencia puede corregir el problema. Esto es una solución fácil y económica que debe probarse primero, porque no requiere la reubicación de ningún equipo.

Si eso no funciona, trate de cambiar la frecuencia de su sistema. Los sistemas en diferentes frecuencias tienden a no interferir entre sí. Una manera fácil de cambiar sus frecuencias es conscientemente cambiar las frecuencias de transmisión y recepción en su sistema.

Detección y solución de problemas de rendimiento de red

Se está tratando de detectar y solucionar problemas en rendimiento de red, lo primero y el mejor consejo es probar laboriosamente y documentar su sistema, el mantenimiento de su configuración y todo lo demás que haga. De esa manera, en caso de que la red empiece a operar de una manera irregular, tiene un historial contra el cual compararlo.

Cambie la administración y su red

Hay dos maneras en que puede detectar y solucionar los problemas de rendimiento de una red. La primera consiste en enfrentarlo, inconsciente de cualquier cambio y modificación que se haya hecho al sistema. Es decir, usted va a corregir el problema, pero no tiene pistas de lo que ya se ha hecho. Cuando esto sucede, lo mejor que puede hacer es empezar por hacer cambios aquí y allá, con base en sus suposiciones educadas y su experiencia, no en los hechos. La segunda y obviamente la mejor solución es reunir información de tendencias de rendimiento básicas y consultar el registro de administración de cambios de la red para que tenga una línea de base funcional a partir de la cual empezar el proceso de detección y solución de problemas.

Un registro de administración de cambios es un documento donde usted registra todos y cada uno de los cambios y la información de mantenimiento que se realice en su sistema, sin importar si son grandes o pequeños. Se instaló un nuevo enrutador, eso debe estar en el documento, pero también debe estar si alguien entró en el cuarto del servidor para restablecer el dispositivo.

NOTA Hay una historia acerca de un técnico de redes que realizó la tarea simple de soplar el polvo de un ventilador de un enrutador. Al final, el polvo entró más adentro del ventilador, causando que se detuviera en intermitentemente y que el enrutador se calentara.

Debido a que el técnico no registró esta tarea "simple" en un documento de administración de cambios, nunca se pensó en revisarse, hasta que fue demasiado tarde y el enrutador se quemó.

También es útil, cuando hagan cambios a la configuración de la red, hacer la menor cantidad de cambios posibles cada vez. De esa manera, si su red tiene algún cambio en el rendimiento o si deja de funcionar por completo, es más fácil deshacer eso que si ha realizado una docena de cosas diferentes.

Si tiene un documento de administración de cambios y sabe cuándo el sistema empezó a tener problemas, puede comenzar a analizar los cambios que se hicieron a la red y sus dispositivos. Podría descubrir que un nuevo protocolo de enrutamiento se introdujo o que una nueva directiva de calidad de servicio se implementó. Si fuera a disparar a ciegas en la oscuridad, le llevaría semanas encontrar estos problemas. Si tiene un documento de administración de cambios, es mucho más fácil detectar el problema.

Un plan de administración de cambios efectivo y bien implementado tiene varios atributos útiles que le ayudarán a su administración general de red y también le ayudarán en la detección y solución de problemas. Entre los beneficios se incluyen los siguientes:

- ▼ Un punto de revisión que le permite medir el rendimiento, antes y después de que se han hecho los cambios en la red.
- ■ Un diario de actualizaciones de red, mantenimientos y reconfiguraciones, que le permiten comparar su red y sus cambios a consideraciones anteriores en la historia de su red.
- ▲ Una herramienta para revertir los cambios, que facilita la restauración de su sistema a una configuración óptima si el rendimiento de una nueva configuración no aviva sus expectativas.

Para obtener mejores resultados, tendrá los dispositivos apropiados de software y hardware que le ayudarán a reunir y analizar las mediciones de rendimiento. Para conocer algunas sugerencias, regresé al capitulo 13.

Problemas de desempeño del enrutador

Si sospecha que hay problemas de desempeño con su enrutador, consulte su documento de administración de cambios. ¿Ha cambiado algo recientemente? Una vez que un dispositivo de red se ha configurado y está trabajando, los problemas generalmente surgen porque una persona está tratando de mejorar el rendimiento del dispositivo. Suponiendo que no hay algún problema de hardware (un cable desconectado o una tarjeta de red insertada de manera inapropiada), entonces el siguiente lugar en que hay que buscar es si se hicieron cambios a la configuración del dispositivo.

NOTA No desechen los problemas de hardware con mucha rapidez. Siempre es posible que alguien haya realizado una tarea aparentemente no relacionada y que por accidente haya jalado un cable de alimentación eléctrica con demasiada fuerza o pinchado un cable de red con un mosaico del piso o la puerta. Inspeccione siempre su hardware antes de que dedique horas a ordenar los archivos de configuración. Uno de los orígenes más grandes de caos en la red lo representan los cables insertados en puertos equivocados. No sienta pena por preparar un mapa que muestra cuáles cables van entre sus

dispositivos y asegúrese de que todos los cables estén etiquetados apropiadamente en ambos extremos para que instantáneamente pueda encontrar donde deben insertarse los cables. Esto es mejor que la opción tediosa: conectar los cables para ver dónde van.

Por suerte, usted creó una copia de seguridad de su archivo de configuración del enrutador, al tomarse unos cuantos segundos para hacer esta copia de seguridad cuando trabajaba en forma óptima finalmente le ahorrará incontables horas tratando de restaurar el sistema. El momento para crear la copia de seguridad del archivo de configuración es cuando todo esté funcionando bien. Las copias de seguridad también deben hacerse antes y después de cada cambio individual al dispositivo. Esto le permite ver exactamente lo que es diferente entre las configuraciones anteriores y posteriores al cambio.

Si no tiene una copia de seguridad del archivo de configuración, el siguiente paso consiste en estudiar la documentación de administración del cambio. Esta documentación debe describir todos los cambios que se han hecho al enrutador. Examine el documento y vea cuáles cambios podrían ser responsables del problema de su enrutador. Tal vez tenga que regresar al archivo de configuración del enrutador y deshacer esos cambios, uno por uno, hasta que el problema se haya resuelto.

NOTA Mejor aún, si no tiene una copia de seguridad del archivo de configuración de su enrutador, deje este libro a un lado y vaya a hacer una. No se preocupe, aquí lo esperamos.

También podrían ser culpables los cambios en el sistema operativo del dispositivo. Se actualizó recientemente su sistema operativo o se aplicó un parche, es un buen lugar para revisar. Antes de agregar los nuevos sistemas operativos o de aplicar parches, debe comprender cómo puede deshacer el sistema operativo y restaurarlo al sistema operativo operacional anterior si algo sale mal. Sin embargo, recuerde que como sea que usted ataque el problema de detección y solución, el objetivo es seguir el cable y rastrear el origen del problema hasta el final.

Tenga en cuenta que lo más importante de hacer cuando se realiza la detección y solución de problemas es avanzar cuidadosa y lógicamente. No cambie varias variables al mismo tiempo. Haga un cambio, observe (sea paciente), documente si es necesario y luego dé el siguiente paso. Arreglar problemas en sistemas complejos se parece más a un proceso que a la suerte. Dicho eso, les deseamos la mejor de las suertes en la detección y solución de problemas y en la vida.

ÍNDICE

A

AAA, 251-81
- cerradura y llave con una base de datos local de usuario, 282-83
- cómo trabaja, 259-60
- controles de autentificación, 253-55
- controles de autorización, 255-56
- controles de contabilidad, 256-57
- listas de acceso dinámico, 281-82
- métodos y tipos, 265-78
- modularidad, 253-57
- panorama general de, 252-53
- pares atributo-valor, 261
- proceso de aprobación, 260-62
- protocolos de autentificación, 262-64
- RADIUS, 257-59, 278-81
- TACACS+, 257-59, 278-81
- tendencias que llevan a sistemas de seguridad cliente-servidor, 257
- transacciones de autentificación, 262
- transacciones de autorización, 262

Acceso
- a la red, 417
- a las LAN, 39
- de sitio a sitio, 328-29

Acceso protegido WiFi (WPA), 362-67

Access Control List (ACL, lista de control de acceso), 90, 292
- reflexivas, 296

Adaptive Security Algorithm (ASA, algoritmo adaptativo de seguridad), 312-18

Adaptive Security Appliance (ASA, aplicación de seguridad adaptativa), 319-21

Administración
- de direcciones, 234-35
- de sistemas corporativos, tendencias en, 529-31

Agregación de datos, 539-41

Almacenamiento adjunto de red, 433-35

Almacenamiento de trabajo, 117

Almacenamiento en caché, 453-64
- actualización de la, 456-57
- confiabilidad, 462-63
- estilo sin transparencia/proxy, 458-59
- estilo transparente/proxy, 457-58
- evitar, 463-64
- grupo, 462
- proxy invertido, 459-60

varios usos del motor de contenido, 460-62
Web Cache Communication Protocol (WCCP), 455-56
Ancho de banda, 4-5, 8, 146, 573-74
para el IOS, 144
Aplicación, 56
firewalls de capa, 298
protocolos, 8
Application and Content Networking System (ACNS, sistema de conectividad de aplicación y contenido), 450-51
Árbol de distribución de transmisión múltiple, 448
Archivo de configuración, 134-36
papel central de, 138-42
tipos de, 156-57
Archivos dinámicos, 140
Arquitecturas, 33-34
de cómputo, 33-34
Ethernet, 40-41
FDDI, 46-47
interconectividad, 578
protocolo de enrutamiento, 495-99
WLAN, 339
ASA de Cisco, 291
ASCII, 264
Asistentes digitales personales (PDA), 15
Asistentes Inteligentes, 106-7
ATM (Asynchronous Transfer Mode, modo de transferencia asincrónica), 17, 26, 39, 41, 44-45, 210, 216, 583, 611
Autentificación, 252
controles, 253-55
métodos, 267-70, 366
protocolos, 262-64
transacciones, 262
Autentificación, autorización y contabilidad. *Véase* AAA
Autoconfiguración inestable, 82
AutoDetect Device Wizard (asistente para autodetección de dispositivo AutoDetect), 178-79

B

Binarios, 30-31, 33
Bits, 30-32, 68
Border Gateway Protocol (BGP, protocolo de gateway de borde), 16, 514-15
Bytes, software operando sobre, 32

C

Cable de par trenzado, 197
especificaciones, 200
Cableado
conectados directamente contra conectados cruzados, 204
de fibra óptica, 196
directo, 204
distancia y velocidad de la red, 196-204
especificaciones, 199
espina dorsal, 197
fibra óptica, 196
LAN, 197-204
par trenzado, 197
Shielded Twisted-Pair (STP, par trenzado con protección), 197
Unshielded Twisted-Pair (UTP, par trenzado sin protección), 199
Calidad de Servicio (QoS), 44, 125, 146, 302, 324, 331, 391, 424, 591-92
Canales, 8, 49
Capas
abstracta, 33
de acceso, 16, 18
Carga de tráfico, 594-95
Carrier Sense Multiple Access with Collition Detection (CSMA/CD, acceso múltiple de percepción de portadora con detección de colisiones), 40
CDDI (Copper Distributed Data Interface, interfaz de datos distribuidos por cobre), 46
CDN, 438-53
Application and Content Networking System (ACNS, Sistema de conectividad de aplicación y contenido), 450-51
cómo trabaja, 439-41
Conmutación de contenido, 445
Content Distribution Manager (administrador de distribución de contenido), 441-43
Enrutamiento de contenido, 443-44
Entrega de contenido en el borde, 444-45
Motores de contenido, 442-43
necesidades de, 438-39
Servicios inteligentes de red, 446
Transmisiones múltiples IP, 446-49
Cerradura y llave, 282-83
CHAP (Challenge Handshake Authentication Protocol, protocolo de desafío de autentificación de saludo), 264
Cheapernet, 197
Ciclos por segundo (CPU), 31
Cifrado, 54, 115, 131, 324, 336, 653-56
Circuito PRI (interfaz de velocidad primaria), 50
Circuitos, 8
análogos/módem, 49
módem, 49
PRI, 50
telefónicos, 12
virtuales permanentes, 53
Cisco
adquisiciones, 21-22, 23-25
archivo de configuración, 134-36
archivos de enrutador, tipos de, 139-42
archivos esenciales, 126-36
conectividad inalámbrica, 350-55
ConfigMaker, 175
conmutadores, 188-242, 205-13, 218-19
enrutadores de espina dorsal, 125-26
Fast Step, 180-86
Internet y, 3-27
la competencia y, 20-21
modelos de enrutador, 122-26
modelos de enrutamiento de alcance intermedio, 124
portafolio, expandiendo el, 22-23
posición en la industria, 6-7
productos de, 19-20
productos de redes conmutadas, 216-18
protocolos de enrutamiento, 503-19
software de, 22
software IOS, 126, 127-34
soluciones de, 25-27
Cisco Discovery Protocol (CDP, protocolo de descubrimiento de Cisco), 15, 165-69, 208, 577
Cisco Fabric Manager, 433
Cisco Group Multicast Protocol (CGMP, protocolo de transmisión múltiple de grupo de Cisco), 236-37
Cisco Network Admission Control (NAC, control de la admisión en la red), 320
Cisco Network Assistant (asistente para redes de Cisco), 555-70

Cisco SAN-OS, 431
Cisco Security Manager (CSM, administrador de seguridad de Cisco), 331-32
Cisco Unified Communications (Comunicaciones Unificadas de Cisco), 400-408
Cisco Unified Presence Server (Servidor de Presencia Unificada de Cisco), 401
Cisco Wide Area Application Engine (WAE, motor de aplicación de área amplia), 451-52
Cisco Wide Area File Services (WAFS, sistema de archivos de área amplia), 452-53
CiscoSecure ACS, 253, 262
CiscoView, 223
CiscoWorks, 132, 555
CLI (command-line interface, interfaz de línea de comando), 431-32
Clóset de datos, 603
Cluster Management Suite (CMS), 218-24
Codificación, 388-91
Community string (cadena comunitaria), 232
Concentradores, 197
Conectividad, 4-6, 415
    aislamiento de problemas de, 625-41
    bases de diseño, 572-88
    definición, 4, 8
    diseñada para satisfacer necesidades, 588-95
    diseño conmutado de, 289-13
    firewalls como seguridad en, 296-97
    jugadores en, 13-14
    modelo de diseño jarárquico de tres capas, 578-83
    panorama general, 4-6
    protocolos de, 14-16
    tendencias de, 17-19
    tipos principales de dispositivos, 8-11
    topologías básicas, 12-13
Conectividad inalámbrica, 19, 27, 47-48, 334-37
    adaptadores de cliente, 355
    adquisiciones de Cisco, 351-54
    detección y solución de problemas, 652-59
    Puente Inalámbrico Aironet de Cisco, 355
Conexión satelital, 51-52
ConfigMaker, 174, 175-80
    ambiente de escritorio, 175
    análisis del producto, 179-80
    construcción de una red con, 178-79
    metodología, 176-78
Configuración
    cadena de, 588
    conmutador-enrutador, 601-9
    contraseñas, 262
    de cadena, 588
    de doble base, 300
    de los puntos de acceso, 355-67
    detección y solución de problemas, 651-61
    doble base, 300
    enrutador, 159-69
    estrella, 191
    puerto conmutado, 226-27
    punto de acceso, 355-67
    registros, 169
    SAN, 417-19
    VLAN Membership Policy Server (VMPS, servidor de directivas de membresía VLAN), 240-42
Conjuntos
    de administración de la seguridad de Cisco, 331
    de características, 127
    de reglas, 305
Conmutación
    basada en el destino, 228
    basada en la fuente, 228
    de capa 3, 213
    de etiquetas de varios protocolos, 515-18
    de varias capas, 212-13, 582
Conmutadores, 5, 8, 188-242
    cableado y, 196-204
    capa 2 de MAC, 576-77
    Catalyst LAN de Cisco, 216-17
    cómo trabajan, 205-6
    con base al destino, 228
    configuración de puertos, 226-27
    configuración y administración, 218-19
    datos, 16
    diseño de conectividad, 289-13
    dispositivos, 211
    en comparación con enrutadores, 16-17
    fundamentos de conectividad, 206-8
    tecnologías de los, 212
    varias capas, 212-13, 427-28
Conmutadores MDS, 421-35
    almacenamiento adjunto de red, 433-35
    Cisco Fabric Manager, 433
    hardware de, 427-31
    interfaz de línea de comando (CLI), 431-32
    MDS 9500 Fabric Switches, 428-29
    MDS 9500 Multilayer Director Switches, 427-28
    módulos, 429-31
    PortChannel, 426
    SAN-OS de Cisco, 431
    software de, 431-33
    SPAN, 425
    tecnologías, 421-26
    troncales, 425-26
    VSAN, 421
Conmutadores para LAN catalyst de Cisco, 216-17
Contabilidad, 252
    aviso de, 276
    controles de, 256-57
    métodos y tipos, 274-78
Contenido multimedia, 19
Context-Based Access Control (CBAC, control de acceso basado en el contexto), 301, 302-4
    recuperación, 173
Contraseñas
    configuración, 262
    Enable y Enable Secret, 115-16
    Enable, recuperación, 170-72
    enrutadores, 112-16
    línea de, 113-15, 173
    protocolos, 262
    recuperación de, 169-74
Contraseñas de línea, 113-15
Control
    administrativo, 289, 499
    de vínculo de datos de alto nivel, 107
Convergencia, 479
CORBA (arquitectura de corredor de solicitud de objeto común), 34
Cuchillas, 123

D

Data Agregation, 539-41
Datagrama, 38, 57
Deliver Configurations Wizard (asistente para configuraciones de entrega), 178, 179
Denial-of-Service (DoS, negación del servicio), 244, 247, 301

Dense wavelenght division multiplexing (DWDM, Multiplexión densa por división de longitud de onda), 96, 97-98
Desktop Aironet Utility (ADU, utilería de escritorio de Aironet), 367
Desviación simple de tarifa, 383-84
Detección de direcciones duplicadas (DAD), 83
Detección y solución de problemas, 618-61
Digital Media System (DMS, sistema de medios digitales), 470-72
Dirección remota, 183
Direccionamiento
de transmisión múltiple, 82
difundido en una dirección, 81
Fast Step, 183-84
tipos de, 81-82
transmisión múltiple, 82
una sola transmisión, 81
Dispositivos, 8, 20
administrado, 531
de acceso, 286
de extremo, 71
estatus, examen del, 165
ventana, 175
Distribución de video, 27
Domain Name System (DNS, sistema de nombres de dominio), 58, 600-601
Dominios, 192-96
Token, 194-95
Dynamic Host Configuration Protocol (DHCP, protocolo de configuración dinámica del host), 206, 358, 599

E

Ejecutables, 33
Empaquetamiento de enrutador, 122
Encuesta de grupo, 532-33, 539-41
Enhanced Interior Gateway Domain Protocol (EIGRP, protocolo mejorado de dominio de gateway interior), 508-10
actualizaciones, 476
bucle, 488-89
Conmutación de etiquetas de varios protocolos, 515-18
cortes de transmisión, 489, 490
demora de propagación, 487-88
envenenamiento de actualizaciones inversas, 489, 492-93
híbrido, 499
horizontes divididos, 489, 490-91
implementación, 499-503
mediciones, 493-94
Open Shortest Path First (OSPF), 511-14
RIP 2, 510-11
tabla, 478-79
vínculo-estado, 496-99
Enrutadores, 5, 10
acceso a, 250, 329-31
acceso administrativo a, 100
aplicaciones para configurar, 174-86
archivo de configuración, 138-42
archivos de Cisco, tipos de, 139-42
comandos, 158-59
comparación entre conmutadores y, 16-17
comunicación, 98-104
conectividad, dispositivo en, 574-75
configuración paso a paso, 159-63
contraseñas, 112-16
de acceso, 250, 329-31
de alcance medio de Cisco, 123
eficiencia, 92-93
empaquetado de, 122
espina dorsal, 123-26
hardware, 116-22
identidad, otorgando, 163-65
Internet y, 93-95
memoria, 117-18
modelos de Cisco, 122-26
modo de operación, configuración de, 160-63
modos, 154-57
ópticos, 95-96
panorama general, 90-135
pequeñas oficinas y oficina en casa (SOHO), 122-23
problemas de desempeño de, 660-61
protección, 291
puertos y módulos, 118-22
seguridad, 110-16
selección de, 119
tamaños de, 95
Enrutadores de Cisco
comandos del IOS, 148-54
comunicación con el IOS, 142
IOS, 143-47
IOS XR, 147-48
modos de operación de, 154
recuperación de la contraseña para, 169
recuperación de la contraseñas de enrutadores anteriores, 173
tipos de, 139-42
Enrutamiento
de alta velocidad, 213
dinámico, 481
distancia-vector, 495-96
estático, 481
híbrido, 499
vínculo-estado, 496-99
Entunelamiento, 327-29
Equilibrio de carga, 585-86
Espacio de direcciones, 597
Espina dorsal
cableado, 197
conmutada, 209-11
de alta velocidad, 609-12
enrutadores, 123-26
FDDI como red, 45
LAN, 39
tecnologías, 17
Estación, 8
Ethernet, 36, 39-40, 121, 201
arquitectura, 40-41
conexión rápida, 162
dominios de colisión, 193-94
estadísticas de, 635-37
Gigabit, 41-42
implementaciones, 41
módulos, 122
segmento LAN de, 40
Ethernet Gigabit, 17, 41-42, 48, 210, 216, 228
Extended ping (ping extendido), 628

F

Fast Ethernet, 162, 210, 216, 228
Fast Step, 174, 180-86
búsqueda y conexión, 180-86
configuración y prueba, 184-85
direccionamiento local, 183-84
revisión del producto, 186
seguridad, 182

FCIP, 415
FDDI (Fiber Distributed Data Interface, interfaz de datos distribuidos por fibra), 35, 45-47
Fiber Distributed Data Interface (FDDI, interfaz de datos distrubuidos por fibra), 35, 45-47
Fibre Channel, 412-15
Firewall PIX de Cisco, 291
Firewall PIX Secure de Cisco, 311-18
    Adaptive Security Algorithm (ASA, algoritmo adaptativo de seguridad), 312-18
    tipos y modelos, 318
Firewalls, 5, 11, 286, 287-89, 291-97
    asistente de, 178, 179
    capa de aplicación, 298
    como defensa, 289
    cómo trabajan los, 291-92
    configuración, 109-10
    definición, 287
    fundamentos, 288-89
    lista de acceso de seguridad, 292-95
    rastrear sesiones de interconexión con, 296-97
    regla de la negación implícita, 293
    seguridad con base en el tráfico, 247-48
Flujo de tráfico, 592-94
Formato de punto decimal, 68
Frame Relay, 53-54, 107, 165, 612-13
Fusión, 25

G

Gateways, 387-88,394

H

H.323, 391-95
Hardware
    detección y solución de problemas, 649-51
    enrutadores de, 116-22
    MDS, 427-31
    para el IOS, 144
    redes privadas virtuales (VPN), 325
Host, 8

I

iFCP, 416
Integración de voz/datos, 26
Integrated Services Digital Network (ISDN, red digital de servicios integrados). *Véase* ISDN
Interconexión de sistemas abiertos (OSI), 34
    implementación, 37-39
International Organization for Standardization (ISO), 34
Internet
    Cisco y, 3-27
    como capa, 56
    definido, 8
    enrutadores y, 93-95
    privado, 71
    tecnologías de, 8
Internet Assigned Numbers Authorithy (IANA), 61, 67, 449
Internet Backbone Providers (IBP, proveedores de espina dorsal de Internet), 14
Internet Control Messaging Protocol (ICMP, protocolo de mensajería de control de Internet), 294
Internet Engineering Task Force (IETF), 15
Interoperabilidad, 34
Intranet, 8
Inundación, 206, 230
IOS, 6, 33, 103, 127-34, 143-47
    comandos de navegación, 159
    comandos, utilización de, 148-54
    comunicación con el, 142
    configuración del firewall, 305-9
    conjunto de características del 301-2
    conjunto de características del firewall de, 26, 127-32
    escritura de comandos del, 153
    funciones del firewall del, 304
    métodos de autentificación de, 268
    modos de configuración del, 154-55
    sintaxis de comandos del, 152-53
    tipos de autorización de, 273
    XR, 148-48
IP
    administración del, 230-31
    clases de direcciones, 69-71
    conmutación, 213
    datagrama de, 57
    dirección, 66-67, 76, 77
    formato de datagrama de, 59-60
    formato de las direcciones, 68
    IP Versión 6, 79-84
    prefijo de, 81
    servicios de, 146
    solución de videoconferencia, 467-70
    telefonía, 19, 403-4
    teléfonos, 387
    transmisión múltiple, 446-49
iSCSI (Small Computer System Interface, interfaz de sistema de computadora pequeña sobre IP), 415
ISDN, 581, 614
ISP (Internet Service Provider, Proveedor de Servicios de Internet), 13, 244, 291
    conectividad, 26

J

Java, 34

L

LAN (red de área local), 8, 90, 165
    acceso a, 39
    cableado, 197-204
    conmutador, 216
    especificaciones, 202-3
    espina dorsal, 39
    inalámbrica, 47-48
    segmento, 8, 9, 12, 40, 43, 191, 291, 572
    topología de la red y, 189
    virtual, 196, 211, 213-15
Línea de base NetSys, 174
Línea de suscriptor digital (DSL), 13, 50-51, 581, 615-16
    asimétrico, 51
    Lite, 51
Líneas arrendadas T1 y T3, 53

Líneas VTY, 103, 113
Listas de acceso dinámico, 281-82

M

Main Distribution Facility (MDF, instalación principal de distribución), 604
Marco, 38
de datos, 39
MARS de Cisco Security, 332
MDS (Multilayer DataCenter Switches, conmutadores de centros de datos de capas múltiples). *Véase* MDS
Media Acces Unit (MAU, unidad de acceso al medio), 42
Media Access Control (MAC, control de acceso al medio), 38, 39, 193
Medio físico de transmisión, 8
Memoria
enrutador, 117-18
estática, 117
flash, 117-18
NVRAM, 117, 156, 161, 164, 204
RAM/DRAM, 117
ROM, 118
Método CSMA/CD (acceso múltiple de percepción de portadora/detección de colisiones, Carrier Sense Multiple Access/Collision Detection), 193
MIB (Management Information Bases, bases de información para la administración), 534-36, 537-39
Módem por cable, 51-52, 616
Módulos de interfaz, 116
MPLS (Multiprotocol Label Switching, conmutadores de etiqueta de multiprotocolo), 19
Multiplex, 49
Multipoint Control Units (MCU, unidades de control multipunto), 394-95
MVS, 6

N

NAT, 72, 297, 575, 648
Network Analysis Modules (NAM, módulos para el análisis de la red), 144
Network Based Application Recognition (NBAR, reconocimiento de la aplicación basada en la red), 146
Network Interface Card (NIC, tarjeta de interfaz de red), 188
Network Management Module (NMM, módulo de administración de red), 229
Números de puerto, 58,61
NVRAM (RAM no volátil), 117, 126, 156, 161, 164, 204

O

Octetos, 68
ejemplo de subred completa, 73-75
subred parcial, 77-78
Open Shortest Path First (OSPF), 511-14
Optimized Edge Routing (OER, enrutamiento optimizado del borde), 145
Ordinalidad, 31
Orientación de circuito virtual, 44

P

PAP (Password Authentication Protocol, protocolo de autentificación de contraseña), 264
Paquetes, 9, 38, 57, 93-94
Paquetes de características, 127
Pares atributo-valor, 261
Paso de fichas, 194
PAT, 72
PBX con capacidades IP, 383
Ping, 626-27, 648
Point-to-Point Protocol (PPP, protocolo punto a punto), 107, 180, 181, 251
Portador óptico, 44,96
PortChannel, 426
Porteros, 394
Procesadores multipunto (MP), 394
Programa de arranque, 118
Protocolo de Árbol Expandido (STP), 221-22, 238-39
Protocolo de Descubrimiento de Gateway, 483
Protocolo de Información de Enrutamiento. *Véase* RIP
Protocolo de Inicio de Sesión (SIP), 15
Protocolo de Internet. *Véase* IP
Protocolo de transferencia de archivos (FTP), 92
Protocolo de transferencia de hipertexto (HTTP), 36
interfaz de usuario del servidor, 104-5
Protocolo Ligero de Presentación (LPP), 36
Protocolos
aplicación, 8
autentificación, 262-64
Cisco Discovery, 165-69
conectividad, 14-16
confiables, 57
contraseñas de, 262
definición de, 14
enrutamiento de, 476-519
Internet, 13
mantenimiento de, 15-16
marcación, 251
protocolo de árbol expandido (STP), 238-39
protocolo de mensajería de control de Internet (ICMP), 294
protocolo de transmisión múltiple de grupo de Cisco (CGMP), 236-37
prueba de extensión, 221-22
RADIUS, 257-59
Resolución de Direcciones, 233
SAN, 415-16
sin conexión, 57
Protocolos de enrutamiento, 476-519
algoritmos, 476
arquitecturas, 495-99
configuración de, 507-8
distancia-vector, 495-96
dominios, 477
enrutamiento dinámico con estático, 481-82
fundamentos, 477-94
la estrategia de Cisco, 503-7, 518-19
Protocolo de gateway de borde, 514-15
Protocolos de marcación telefónica, 251
Prueba de reinicio, 651
Puerta trasera, 588
Puerto consola, 100-101
Puertos, 37
agrupamiento de, 228
auxiliares (AUX), 101, 142
configuración de conmutadores en, 226-27
conmutados, 226

consola de, 100-101
enrutador de, 118-22
red de, 230
seguridad en, 235-36, 424
supervisión de, 229-30
Pulse Code Modulation (PCM, modulación del código de impulso), 389

R

RADIUS, 257-59, 265
atributos, 278-81
RAM/DRAM, 117
Recuperación de fallas, 228
Recuperación de las Enable Passwords, 170-72
Red confiable, 289
Red de área de almacenamiento (SAN), 26-27, 411-20
administración, 419-20
almacenamiento, 411-12, 420
canal de fibra, 412-15
configuración, 417-19
diseño y construcción, 416-20
FCIP, 415
iFCP, 416
iSCSI, 415
respaldo, 420
Red de campus, 601-16
Red desconocida, 289
Red no confiable, 289
Redes
administración, 17, 26, 522-70, 548-52
aparatos, 311
campus, 601-16
caracterización, 591-95
conexión, 36
confiables, 289
de contenido, 27
desconocidos, 289
detección y solución de problemas, 618-49
diseño, 596-616
dominios, importancia de los, 192-96
elemento, 531
empresa, 198
especificaciones, 199
fundamentos, 206-8
inalámbricas, 19
interfaz, 56
necesidad de segmentar, 196
no confiables, 289
puerto, 230
seguridad, 17, 246-51
servidores de acceso a, 249
tecnologías, 8
velocidad y distancia, cableado y, 196-204
VoIP, 382-84
Redes de Entrega de Contenido. Véase CDN
Redundancia, 585-86
Registro de eventos, 300-301
Regla del primer octeto, 69
Remote Procedure Call (RPC, llamada a procedimiento remoto), 36
Repetidores, 197, 341
Respaldos, 135
SAN, 420
RIP, 503-4
RIP 2, 510-11
RMON (supervisión remota), 229, 545-48, 552-55
ROM, 118,126
Ruteador escudo, 291
Ruteo del camino corto, 213

S

SAN. *Véase* Red de área de almacenamiento
SCCP, 397
Scientific-Atlanta, 22, 465-66
Secure Shell (SSH), 102, 142, 618
Security Device Manager (SDM, Administrador de Dispositivos de Seguridad), 105-10, 174
Asistentes Inteligentes, 106-7
configuración del firewall, 109-10
supervisión y reparación de fallas, 108-9
Security Set Identifiers (SSID, identificadores para el conjunto de seguridad), 360
Seguridad, 26,286-332
Adaptive Security Appliance (ASA, aplicación de seguridad adaptativa), 319-21
Algoritmo de seguridad adaptativo, 312-18
basada en el tráfico mediante listas de acceso, 247
basada en el usuario, 244,246,248-49
basada en tráfico, 244,246,248-49
cliente-servidor, tendencias que conducen a, 257
como política, 290-91
configuración de doble base, 300
configuración del firewall IOS, 305-9
Conjunto de administración de la seguridad de Cisco, 331-32
Control de acceso basado en el contexto, 302-4
direcciones globales para esconder la topología, 297
enrutador, 110-16
enrutadores de acceso, 329-31
express, 360-62
Fast Step, 182
Firewall basado en tráfico, 247-48
firewall del IOS, 301-2, 304, 309-10
Firewall PIX Secure de Cisco, 311
IOS, 147
lista de acceso, 247, 292-95
MARS de Cisco Security, 332
MDS, 424-25
panorama general, 244-83
protocolos de marcación, 251
puertos, 235-36
Punto de Acceso, 361-62
RADIUS, 257-59
red, 17
red privada virtual (VPN), 322-29
registro y notificación de eventos, 300-301
servidores de acceso, 249-51
servidores proxy, 298-300
SNMP, 550
TACACS+, 257-59
WLAN, 349
Servicio de troncales, 425-26
Servicios inteligentes de red, 446
Servidores, 388
acceso a, 9,249-51
acceso a la red, 249
comunicación de, 249
de acceso, 5, 9, 249-51
de comunicación, 249
HTTP, 104-5
proxy, 298-300
Sesiones medio abiertas, 309

Shielded Twisted-Pair (STP, par trenzado con protección), 197
Shortest Path First (SPF, primero el vínculo más corto), 496
Signal Transfer Protocols (STP, protocolos de transferencia de señal), 388
Simple Mail Transfer Protocol (SMTP, protocolo de transferencia de correo simple), 36, 61
SIP, 395-97
    soporte, 402
Sistema de distribución, 346
Sistema operativo de conectividad (IOS), 20
Sitios remotos, 612-16
SLIP (Serial Line Internet Protocol, protocolo Internet de línea serial), 251
SMTP (Simple Mail Transfer Protocol, protocolo de transferencia de correo simple), 298
SNMP (Simple Network Management Protocol, protocolo simple de administración de redes)
    agregación de datos, 539-41
    comandos, 542
    configuración, 231-32
    definición, 531
    encuesta, 532-33, 539-41
    eventos y trampas, 543-45
    independiente de la máquina, 536-37
    MIB, 533-36, 537-39
    objetos administrados, 532-33
    umbrales, 542-43
Software, 22
    bytes, 32
    compilación, 32-33
    imágenes, 127
    MDS, 431-32
    Software del Cluster Management Suite, 222
Solución de video de negocios de Cisco, 466-67
SONET (Red Óptica Sincrónica), 44, 97
SPAN (Switched Port Analyzer, analizador de puertos conmutados), 229, 425
Subnet, 73-78
    subnet parcial en octetos, 77-78
    máscaras de subred, 75-77
    ejemplos completos de una subred en octetos, 73-75
Subnetwork Access Protocol (SNAP, protocolo de acceso a la subred), 165

T

Tabla ARP (Address Resolution Protocol, protocolo de resolución de direcciones), 233
TACACS+, 257-59
    atributos, 278-81
    no confiables, 57
    paso de ficha, 42
    Protocolo de control de transmisión (TCP), 294
    Protocolo de datagrama de usuario (UDP), 294
    Servidor de Política de Membresía VLAN, 222
    Solicitud de VLAN, 222
    Troncal VLAN, 222
Tamaño de palabra, 32
TCP (protocolo de control de la transmisión)
    establecimiento de una conexión, 64
    formato del segmento, 63-64
    ventaneo, 65-66
TCP/IP (Transmission Control Protocol/Internet Protocol, El protocolo de control para la transmisión/protocolo Internet), 8, 13, 55-61,91
    contra UDP como protocolos de transporte, 57-59
    mensajería, 57
    redes, 111
Tecnologías de marcado telefónico, 48, 49-52
    DSL, 50-51
    ISDN, 49-50
    módems por cable, 51-52
Tecnologías operacionales, 8
Tecnologías ópticas, 97-98
Tecnologías para la habilitación compartida, 13
Telefonía IP total, 383
Telnet, 38,99, 102-3
TFTP (Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos), 132-34, 241
Thicknet, 189
Time-division multiplexing (TDM, multiplexión por división de tiempo), 53, 383
Tipo de conexión, 269-70
Token Ring, 36, 42-44, 193, 194
Topologías de red, 189-204
Topologías
    definición, 189
    direcciones globales para esconder, uso 297
    en conectividad, 12-13
    en estrella, 42
    en estrella jerárquica, 191, 192
    en red, 586-88
    factores de diseño, 193
    red, 189-204
    vista, 224-25
Transmisión, 393
    dominios de, 195-96, 573
    umbrales de tormenta, 230
Transmission Control Protocol (TCP, protocolo de control de transmisión), 294
Transporte, 56
    capa de, 61-66
Trivial File Transfer Protocol (TFTP, protocolo trivial de transferencia de archivos), 58
Troncales, 48
    WAN (red de área amplia), 17, 18, 52-54

U

UDP (User Datagram Protocol, protocolo de datagrama de usuario), 57-59, 62, 66, 294
Uniform Resours Locator (URL, localizador uniforme de recursos), 66
UNIX/LINUX, 6, 102, 160, 311, 453
Unshielded Twisted-Pair (UTP, par trenzado sin protección), 199

V

Ventana Connections, 175
Ventaneo, 65-66
Vidrio, 196
Vínculo, 220
    de telecomunicaciones, 12
    virtual, 36
Virtual LAN (VLAN, LAN virtual), 196, 211, 213-15
    membresía, 239-40
Virtual Private Networks (VPN, redes privadas virtuales), 17, 54, 286, 322-29, 438
    cliente-servidor, 646-49
    componentes de, 324

composición de, 322-25
Virtual Switch Manager (VMS), 218, 219, 221
VMPS (VLAN Membership Policy Server, servidor de directiva de membresía VLAN), 222
configuración de, 240-244
VoIP, 15, 20, 21, 27, 380-95
calidad de servicio, 391
codificación de, 388-91
cómo trabaja, 381-82
construcción de redes, 382-84
gateways, 394
H.323, 391-93
implementación de, 397-400
implementación de sucursales, 399-400
porteros, 394
solución, 385-88
terminales, 393
unidades de control de varios puntos, 394-95
Voz sobre IP. *Véase* VoIP
VQP (VLAN Query Protocol, protocolo de consulta de las VLAN), 222
VSAN, 421
VTP (VLAN Trunk Protocol, protocolo de troncales VLAN), 222
administración de, 240

W

WAN (red de área amplia), 13, 48, 90, 286, 323
detección y solución de problemas, 641-46
módulos de conectividad para, 122
tecnologías de, 48-54
troncales, 17, 18, 52-54
Web Cache Communication Protocol (WCCP, protocolo de comunicación de la caché de Web), 455-56
Wintel, 6, 34, 36
Wizards (Asistentes)
Configuración de Entrega, 178, 179
Dispositivo AutoDetect, 178-179
Firewall, 178, 179
WLAN (red de área local inalámbrica), 334, 337-50
arquitectura, 339
cómo trabajan, 337-339
controladores, 351
de igual a igual, 340
edificio a edificio, 342
en un edificio, 340-342
precio de, 350
seguridad en, 349
tecnologías de, 342-348
WPA, 362-67